Informazio Sistemen Segurtasuna Kudeatzeko Sistemak 2025/2026

Zifraketa II

Helburuak:

1. PGP (OpenPGP, GnuPG) motako tresnak erabiltzen ikastea, komunikazioak seguruago bihurtzeko.
2. Konfidantza eraztunei buruz ikastea.
3. GPG-ek eskaintzen dituen beste funtzioei buruz ikastea.

Beharrezko baliabideak:

- Ubuntu (lsi/lsi).

Aurkibidea:

1. GPG bidez komunikazioak seguruago bihurtu.
2. Gakoenganako konfidantza.
3. Gakoen eraztun publikoak.
4. ISSKS klaseko gakoen eraztuna.
5. GPG sinadurak.
6. GPG-ren beste funtzio batzuk.

GPG bidez komunikazioak seguruago bihurtu

GnuPG[1] (GPG) programa librea da, informazioa zifratu, deszifratu eta sinatzeko balio duena, OpenPGP[2] estandarra jarraituz. Gure komunikazioak seguru bihurtzen ditu. Linux distribuzio gehienek GPG daukate, baina Ubuntu-n horrela instalatu ahal da:

```
$ sudo apt install gpg
```

GPG-k aukera asko eskaintzen ditu. Komenigarria da aukera horiek ikustea:

```
$ gpg --help
```

GPG-rekin lan egiteko, lehenengo gako bikotea sortu behar dugu (Pribatua eta publikoa):

```
$ gpg --generate-key
```

Oso garrantzitsua da baleko email bat sartzea. Gako-esaldia aukerakoa da, eta giltzarrirako sarbidea gako pribatuetatik babesteko balio du. PGPn, giltzarria erabiliko

1 https://gnupg.org/
2 https://www.openpgp.org/

diren gakoak biltegiratzen diren biltegia da. Giltzarri pribatu bat dago, eta gako publikoen giltzarri bat. Giltzarria esaldi batekin babestea gomendatzen da.

`gpg --full-generate-key`, komandoaren bidez zer gako-luzera erabili nahi duzuen eta hori sortzeko zer algoritmo erabili nahi duzuen adieraz dezakezue. GnuPG-k RSA, DSA eta ElGamal dauzka. Gako parea sortzeko entropia izeneko neurri bat erabiltzen da, gakoak duen ausazkotasun edo desorden maila adierazten duena. Zenbat eta entropia handiagoa, orduan eta ausazkotasun handiagoa eta, beraz, kriptoanalisia egitea zailagoa. Klabeak sortzean, makinaren datuetan oinarrituta lortzen da entropia, hala nola PUZ (CPU)-aren egoera, data, irekitako leihoen kopurua, etab. Horrela, gakoa sortzen den bitartean, komeni da nabigatzea, leihoak irekitzea, gauzak tekleatzea eta abar, ahalik eta entropia handiena sortzeko.

Gakoak sortu ondoren, gakoak baliogabetzeko ziurtagiri bat sortzeko aukera ematen da. Errebokazio-ziurtagiriak zure gakoa jada ez dela baliozkoa, galdu egin duzulako, lapurtu egin dizutelako eta abar adierazteko balio du. Sortu errebokazio-ziurtagiria eta gorde.

Behin gakoak sortuta, ikusteko:

```
$ gpg --list-keys
```

¿Zer esan nahi du **[ultimate]**-k?

Gako publikoa eskuragarri egotea garrantzitsua da. Web orrialde batean argitaratu daiteke[3], email batean atxikia bidali daiteke, edo **keys.openpgp.org** bezalako zerbitzari batera igo daiteke (Ikus atala aurrerago).

GPG Thunderbird bezalako email bezeroen bidez erabili daiteke, edo terminalean zuzenean. GPG bidez terminalean zifratuak izan diren artxiboak bidaltzeko email-ean atxikitzea nahikoa da.

- PDF artxibo hau zifratu eta zuen artean bidali hurrengo printzipioak lortzeko: **Konfidentzialtasuna, Osotasuna, Kautotzea** eta **Zapuztezintasuna**.

Arrazoitu zer egin behar izan duzuen horietako bakoitza lortzeko.

Gakoen konfidantza

Ikusi duzuenez, oso erraza da gako pare bat sortzea eta edozein izen jartzea. Ez da inolako egiaztapenik egiten. Beraz, Xk sinatutako eta/edo zifratutako mezu bat jasotzen badugu, ezin dugu ziurtatu benetan X denik, Xri galdetzeko moduren bat ez badugu behintzat, ea hori den benetan gakoa. Hala ere, pertsona baten gakoetan konfiantza izateko mekanismoak badaude, nahiz eta pertsona hori ezagutu behar izan ez, edo pertsona horrekin hitz egin ez, haren gakoa den egiaztatzeko.

3 Por ejemplo: https://mikel-egana-aranguren.github.io/about/

- Talde bakoitzean ikasle bat “Konfidantzazkoa” bezala hautatu. Alegia, irakasleak pertsona horrengan konfidantza edukiko du. Ikasle horrek bere gako publikoa irakasleari bidaliko dio. Taldeak lortu beharko du beste ikasleek irakasleari bidalitako gako publikoak irakaslearen ordenagailuko gakoen eraztunean konfiantzazkoak bezala (**[full]**) agertzea.

Arrazoitu hori lortzeko eman behar izan dituzuen urratsak.

Gakoen eraztun publikoak

Gakoak argitaratzeko eta bilatzeko errezena https://keys.openpgp.org/ zerbitzua erabiltzea da. Zerbitzua GPG-en erabiltzeko hurrengo lerroa gehitu behar zaio **/home/{erabiltzailea}/.gnupg/gpg.conf** fitxategiari:

```
keyserver hkps://keys.openpgp.org
```

- Konfiguratu GPG **keys.openpgp.org** zerbitzua terminalean erabili ahal izateko.
- Zure gakoa zerbitzarira igo GPG terminalean erabiliz.
- Irakaslearen eta beste ikasleen gakoak bilatu GPG terminalean erabiliz.
- **Gakoen konfidantza** ataleko ariketa berriro egin, baina gakoak irakasleari bidali beharrean gakoen zerbitzaria erabili terminalaren bidez (Esan irakasleari berak konfidantzazko gakoak bilatzeko).

ISSKS klasearen gako-eraztuna

Aurreko ataleko gako-eraztuna berregingo dugu, baina soilik klaseko ikasleen gakoekin eta eGela erabiliz. Horretarako, irakasleak konfiantza-kate bat izendatuko du ikasle jakin batzuk izendatuz, eta gainerako ikasleek beren gako publikoak igoko dituzte konfiantza batetik bestera hedatuz (Konfiantzazko ikasleetatik hasita). Irakasleak katearen konfiantza egiaztatuko du gako guztiak inportatuz, baina konfiantza azkenari soilik emanez (Inportatzean, denak konfiantzazko gisa agertu beharko lukete irakaslearen ordenagailuan).

GPG sinadurak

Enigmail garatzaileen orrialdean[4] bi fitxategi deskarga daitezke: Thunderbird-erako luzapena (.xpi) eta “GPG Signature” izeneko beste fitxategi bat.

Zertarako balio du bigarren fitxategi horrek? Nola erabiltzen da?

4 http://www.enigmail.net/download

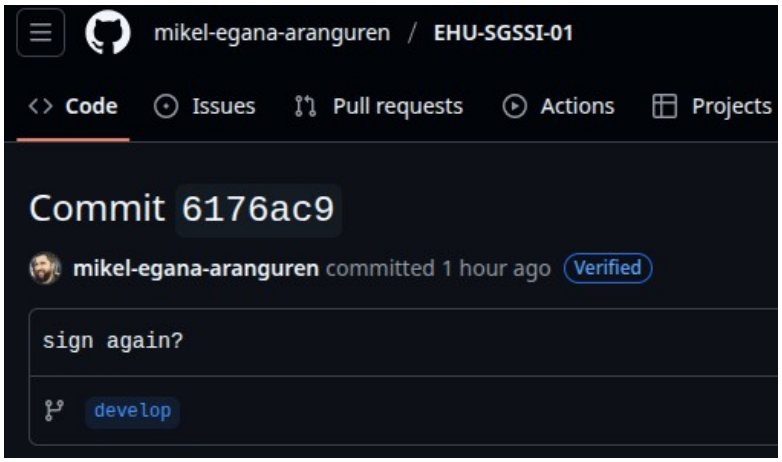
GitHub-en commit-ak sinatzeko aukera dago, commit horien segurtasuna eta jarraigarritasuna hobetzeko. Irakasleak EHU-SGSSI-01[5] apunteen errepositorioaren develop adarreko 6176ac9c479797c698b153c7750fa3e4421f445d hash-a duen commita sinatu du, gako publiko honeri dagokion gako pribatuarekin (mikel.egana.aranguren@gmail.com):

-----BEGIN PGP PUBLIC KEY BLOCK-----

mDMEaMlpKBYJKwYBBAHaRw8BAQdA9BUe340yfVTGvu5htYNgujz5pGtx6GfIRP8h
CALZ+im0OE1pa2VsIEVnYcOxYSBBcmFuZ3VyZW4gPG1pa2VsLmVnYW5hLmFyYW5n
dXJlbkBnbWFpbC5jb20+iJkEExYKAEEWIQQYFaxDxNCAFSKkZypj4GjUA79N7wUC
aMlpKAIbAwUJBaOagAULCQgHAgIiAgYVCgkICwIEFgIDAQIeBwIXgAAKCRBj4GjU
A79N75+fAQD75ya26vOiPsP18zWcclNbEqbt4f/260ycrRYsAoeNAgD/Wsa8GlSP
DnG2X1SC2GY8/X0rfcavzE3Ib4gJzoOkSQe4OARoyWkoEgorBgEEAZdVAQUBAQdA
4zlL3S3rbtPiUuPBscGteaVhYCRjmVuph+0KE/FUQUoDAQgHiH4EGBYKACYWIQQY
FaxDxNCAFSKkZypj4GjUA79N7wUCaMlpKAIbDAUJBaOagAAKCRBj4GjUA79N71q2
AP0W791v7y2QBsaxNuWlZqW/CNHamHJz1hr7tCWs/Jfa2wD9Gh1rszwCy6zXCNOv
hqLrPTy2euh/O45VyZSigvW+QgM=
=aYb8
-----END PGP PUBLIC KEY BLOCK-----

5 https://github.com/mikel-egana-aranguren/EHU-SGSSI-01

Commit hori GitHub-en egiaztatuta agertzen da (“Verified”). Horrek zer esan nahi du?



Commit hori zure ordenagailu lokalean balioztatu. Ze pausu jarraitu dituzu?

Erabili zure GPG gakoak zure GitHub errepositorio publiko batetako commit bat sinatzeko, GitHub-en ikustean "Egiaztatua" ager dadin. Egiaztatu beste ikasleek sinatutako commitak.

GPG-ren beste funtzio batzuk

Garrantzitsua da zuen klabeak beste ordenagailu batean erabiltzen gai izatea.

Nola exportatzen da GPG gako bat beste ordenagailu batean erabiltzeko?

Gerta liteke gako batek segurtasuna galtzea.

Zelan errebokatuko zenuke zure gakoa?

GPG-ren funtzio nagusia enkriptazio asimetrikoa den arren, enkriptazio simetrikoa egiteko gai da.

Zelan zifratuko zenuke dokumentu hau, eta zein pausu jarraituko zenituzke hartzaileak berau deszifratzeko?