Ana Zelaia Jauregi
EHUko Donostiako Informatika Fakultateko irakasle eta ikertzailea

Kriptografia: komunikazioen pribatutasuna babesten

Aro digitalean murgildurik gaude erabat. Gure artean komunikatzeko Internet eta telefono bidezko komunikazio-sistemak erabiltzen ditugu; lagunekin hitz egiteko edo elkarren artean argazkiak eta bideoak trukatzeko telefono mugikorra erabiltzen dugu naturaltasun osoz. Izan ere, erosoak gertatzen zaizkigu azken urteotan garatu diren aplikazioak eta geure egunerokotasunaren parte bilakatu dira.

Whatsapp edo haren antzeko aplikazioei esker lagunak gertu ditugula sentitzen dugu, haiekin komunikatzen gara, baina bakarrik gaude? Pribatua al da komunikazioa? Telefono mugikorra gurea da, baina ez gure mugikorretik lagunaren mugikorrera iristeko behar diren zerbitzari, wifi-sare edo Bluetooth moduko teknologiak. Zerbitzu horiek beste batzuen esku daude, eta, gure mezuak babestu ezean, komunikazioaren pribatutasuna arriskuan dago.

Mugikor bidezko komunikazioen pribatutasuna babestea oso garrantzitsua da adierazpen askatasunerako eskubidea bermatu nahi bada. Tamalez, pribatutasun hori ez dago bermatuta. Snowdenek 2013an argitara emandako dokumentuek erakutsi zutenez zelatariza modu masiboan egiteko programak existitzen dira. Oihartzun handikoa izan zen baita 2015eko San Bernardinoko hilketaren inguruan Apple etxeak FBIrekin izan zuen auzia; FBIk iPhone bateko informazioa lortzeko laguntza eskatu zion baina Apple enpresak ukatu egin zion, hala eginez gero gainerako iPhone guztien segurtasuna arriskuan jarri beharko zuela argudiatuz. Dela terrorismotik babestu beharra argudiatzen delako, dela hainbat enpresek datuen ustiaketarekin dituzten interes ekonomikoen alde dihardutelako, komunikazio-sistemen pribatutasuna arriskuan dago.

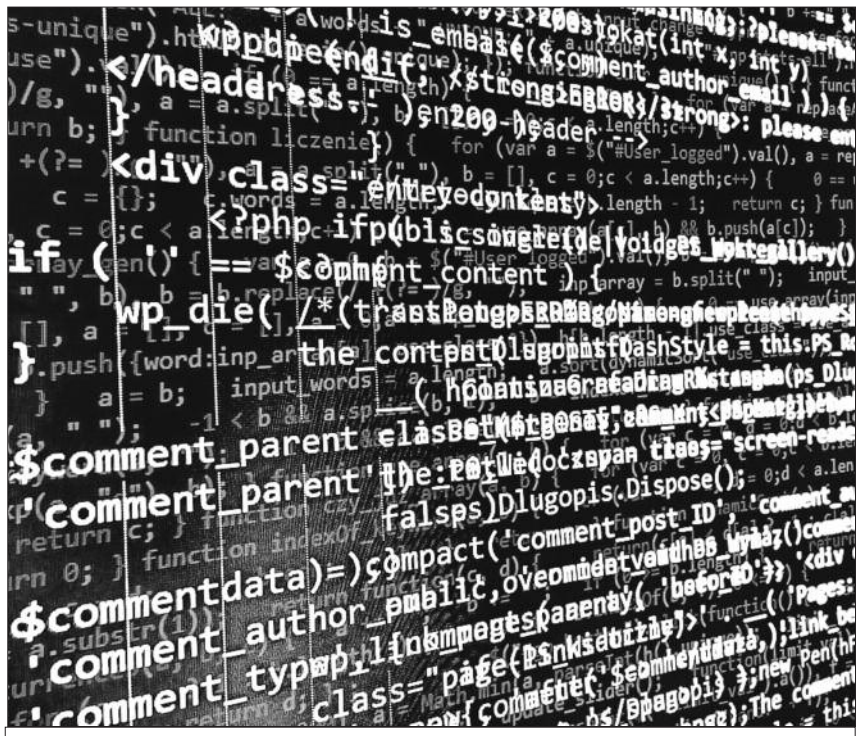
Nazio Batuen Erakundeak 2014an "The Right to Privacy in the Digital Age" izenburupean argitaratutako txostenean estatuei komunikazioen pribatutasunaren alde egiteko eskatzen die, baita Internet bidezko komunikazioetan ere. Berriki, 2016ko urrian, Amnesty International gobernuz kanpoko erakundeak teknologia alorreko 11 enpresaren sailkapena egin du "For your eyes only? Ranking 11 technology companies on encryption and human rights" txostenean. Sailkapenaren lehen postuan ageri da Facebook enpresaren Whatsapp aplikazioa eta atzetik baina gertu Apple etxearen iMessage eta Telegram Messenger. Azken batean, teknologia enpresek sortu behar dituzte txostenek jasotzen dituzten eskubideak bermatuko dituzten aplikazio informatikoak.

Whatsapp eta bere fundatzaileak pribatutasuna babestearen alde agertu dira. Apple berari publikoki babesa erakutsi zioten FBIrekin zuen gatazka sutsuen zegoen garaian. Aurten, 2016ko apirilean, zifratze-sistema txertatu du aplikazioan, haren bitartez bidalitako mezuak, argazkiak, bideoak, fitxategiak eta deiak zifratzeko.

Aipatutako zifratze-sistema *end-to-end encryption* edo "muturretik muturrerakoa" da, mezua bidaltzailearen mugikorretik ateratzen denetik hartzailearenera iristen den arte zifratuta doalako. Bidean egon litezkeen zelatariek, Internet hornitzaileek edo mezularitza-zerbitzua eskaintzen duen enpresak berak ezingo dute mezua deszifratu, horretarako behar diren gakoak komunikatzen diren bidaltzailearen eta hartzailearen telefonoetan baitaude. Gako horiei esker lortzen da trukatutako mezuen pribatutasuna bermatzea. Whatsapp aplikazioko zure kontakturen batekin komunikatzeko daukazun gakoa ikusi nahi duzu? "Encryption" atalean sakatu eta ikusi!

Whatsapp aplikazioaren zifratze-sistema hainbat funtzio eta algoritmo kriptografikoetan oinarritzen da. Erabiltzen duen Java/Android liburutegia (Signal Protocol library) kode irekikoa da (Open Source) eta eskuragarri dago ikusi nahi duen edonorentzat (*https://github.com/whispersystems/libsignal-protocol-java*). Open Whisper Systems enpresak garatutako softwarea da.

Kriptografia matematika eta ingeniaritza informatikoa elkartzen dituen jakintza-arloa da. Egia esan, mezuak zifratzeko saiakerak ez dira gaur egungo kontua. Kriptografia klasikoaren hasiera duela 4.500 urte inguru kokatzen da. Hala ere, bizi dugun aro digitalak zifratze-sistema berrien beharra sortu du eta gaur egun, erabateko pribatutasuna bermatzen duen sistemarik existitzen ez bada ere, hura lortzeko eman diren urratsak nabariak dira, oztopoak oztopo. •



Mezuak zifratzeko saiakerak ez dira gaur egungo kontua, aspalditik datoz. GAUR8