ANAIA HANDI DIGITALA

Igor Leturia Azkarate
Informatikaria eta ikertzailea

Poliki-poliki eta ia oharkabean, gure komunikazioak, tramite administratibo eta finantzarioak eta beste gauza ugari ordenagailu eta Internet bidez egitera pasatu gara. Beti izan gara jakitun horrek gure pribatutasuna arriskuan jar zezakeela, komunikazio eta datu digital horiek baliabide informatiko ahaltsuak dituztenek —gobernuek, alegia— errazago eskuratzeko moduan jartzen ari ginela. Baina sinetsi nahi izan dugu herritarron zerbitzura dagoen administrazioak pribatutasunerako eskubidea errespetatuko zuela. Bada Edward Snowden AEBko CIA eta NSA agentzietako langile ohiak azken hilabeteotan agerian utzitakoek berretsi digute aspalditik Anaia Handiaren kontrolpean bizi garela.

Aurtengo lehen seihilekoan zehar, Interneteko komunikazioen segurtasunari buruzko hiru artikulu idatzi ditugu, eta argitu dugu nola berma ditzakegun konfidentzialtasuna, autentifikazioa eta anonimotasuna. Jende gehienak ez ditu erabiltzen horietan azaldutako metodo aurreratuak Interneten modu erabat anonimoan nabigatzeko, mezu elektronikoak digitalki sinatzeko edo enkriptatzeko. Baina behintzat badakigu pasahitzak edo kontu korrontearen zenbakiak eskatzen dituzten web-zerbitzuek, posta elektronikoak bidaltzea ahalbidetzen duten web-zerbitzuek, edo telekonferentzia-programek kriptografia erabiltzen dutela gure komunikazio horien pribatutasuna bermatzeko. Zehazki, kriptografia asimetrikoa edo gako publiko bidezko kriptografia erabiltzen da normalean, oso segurutzat hartzen dena, eta horrek ziurtatzen du hirugarrenek ezingo dituztela komunikazio horiek atzeman eta gure informazioa eskuratu.

SNOWDENEK AGERIAN UTZITAKOAK: PRISM, XKEYSCORE, TEMPORA...

Edozein hirugarrenek ez, baina gobernuak ez dira edonor. Baliabide gehiago dituzte, eta ez informatikoak soilik. Kriptografia-metodo horiek hausten saiatu beharrean, errazago zaie zerbitzu horiei zuzenean eskatzea. AEBko CIA eta NSA informazio- eta segurtasun-agentzietako langile ohiak, Edward Snowdenek, aurtengo maiatzean eman zien PRISM programaren berri *The Guardian* eta *The Washington Post* egunkariei, NSAko barne-transparentzia batzuekin frogatuta, eta ekainean argitaratu zuten haiek. Programa horren bidez, Interneteko 9 enpresa handiren bezeroen datu guztietarako sarbidea lortzen omen du 2007tik NSAk. Eta enpresa horiek ez dira edozein: Microsoft, Yahoo!, Google, Facebook, Paltalk, Youtube, AOL, Skype eta Apple (eta Dropbox programan laster sartzekotan omen zen).

Enpresa horiek guztiek ukatu egin dute bezeroen datuak NSAri ematen dizkiotela. Baina AEBko gobernuak programaren existentzia ziurtatu du: batetik, Snowden auzitara eraman du espioitza eta gobernuaren jabegoaren lapurreta karguak leporatuta (Errusiak asilo politikoa eman dio, eta han bizi da egun); bestetik, herritarrak lasaitu nahi izan ditu, esanez atzerritarren komunikazioak irakurtzeko soilik erabiltzen dela.

Ekainean, Snowdenek Tempora programaren berri eman zuen, *The Guardian*en bidez. Programa hori Erresuma Batuko GCHQ segurtasun-agentziaren (NSAren parekoa) programa da, PRISM programaren antzekoa: hiritarren komunikazioak eta informazioa biltzen ditu. Gainera, gero NSAri ematen omen diote informazioa. Eta uztailan eta abuztuan, XKeyscore sistemaren berri eman zuen Snowdenek *The Sydney Morning Herald* eta *O Globo* egunkarietan argitaratutako artikulu banaren bidez. NSAren software horrek aukera ematen du atzerritarren Interneteko datu eta informazioak bilatzeko eta aztertzeko. Eta Australia eta Zeelanda Berriko gobernuek ere parte hartzen omen dute.

ARG.: © LIGHTWISE/123RF

ESPEKULAZIO UGARI

Snowdenen filtrazioek soka luzea ekarri dute. Maiatzetik hona hilero eman du argitara eskandalu berri bat Snowdenek berak; baina behin hautsak harrotuta, badirudi paranoia zabaldu dela, eta beste espekulazio ugari ere aireratu dituzte komunikabideek gaiaren inguruan.

Ikusirik NSAk PRISM programako enpresa handi horien guztien datuetarako sarbidea duela eta enpresok informazioa ematen diotela ukatzen dutela, zurrumurruak zabaldu ziren irailean, zeinek baitzioten agian NSAk huts bat aurkitu zuela gako publikoen bidezko kriptografian eta horretaz baliatzen zela HTTPS bidezko trafikoa desenkriptatzeko. Hori egia balitz, hau da, benetan gako publiko bidezko kriptografian huts bat balego, eta huts hori ezagun bihurtuko balitz, eta huts horretaz probesteko beharrezko baliabideak edonork edo ia edonork (eta ez bakarrik NSAk) eskuratzeko modukoak balira, benetan ikaragarria litzateke: webeko komunikazioen konfidentzialtasuna ezingo litzateke bermatu, edonork ikusi ahal izango lituzke pasahitzak, kontu korronteen zenbakiak eta mezuak… Ezagutzen dugun weba desagertu egingo litzateke.

Zorionez, badirudi ez dela horrela. Hainbat arrazoi daude pentsatzeko gako publikoen bidezko kriptografia segurua dela, eta horren inplementazio jakin batzuen hutsez edo konpainia batzuen praktika okerrez baliatuz lortzen duela informazioa NSAk (adibidez, hutsak aurkitu ondoren konpondu diren softwareen bertsio zaharrak erabiltzea, gako laburregiak erabiltzea, edo gako pribatuak modu ez nahikoa seguruan gordetzea); gauzak ongi eginez gero, metodoak segurua izaten jarraitzen du. Gainera, enpresek informazioa borondatez entregatzeak eta gezurretan aritzeak aukera askoz probableagoa dirudi, kriptografia asimetrikoa hautsi izanak baino. Horrela ez balitz, ez lirateke ibiliko beste enpresa askori ere datuak eskatzen.

Irailean zabaldutako beste zurrumurru batek zioen beharbada NSAk nolabaiteko atzeko ate bat ireki zuela Linux sistema eragilearen (Interneteko zerbitzarietan gehien erabiltzen dena) ausazko zenbakien sorkuntza-metodoan. Gako publikoen bidezko kriptografian, gako pribatua ausaz lortutako bi zenbaki lehenek osatzen dute. Erabateko ausazkotasun informatikoa ezinezkoa da, baina orokorrean badira nahiko ausazkotasun handia lortzeko moduak, eta horiek erabiltzen dira kriptografian. Hala ere, ausazkotasun hori murriztuko balitz, edo ausazkotasun horrek patroi ezagun batzuei erantzungo balie, errazagoa litzateke gako pribatu bat asmatzea.

"Enpresek informazioa borondatez entregatzeak eta gezurretan aritzeak aukera askoz probableagoa dirudi, kriptografia asimetrikoa hautsi izanak baino"

> *"Komunikazio digitalak atzitzea pribatutasuna larriki haustea da; mundu analogikoan, gutunak ireki eta irakurtzearen edo telefono-deiak ziztatu eta entzutearen parekoa"*

Linuxen kolaboratzaileetako batzuek kezka agertua zuten Linuxen ausazkotasun-iturrietako bat RdRand izan zitekeela, ausazko zenbakiak Intel mikroprozesagailuan hardware bidez sortzen dituen funtzioa. Haien ustez, ausazko zenbakien sorkuntza hardware bidezkoa zenez, ezin zen ikuskatu eta ikusi ea esaten zuena egiten zuen benetan. PRISM eta abarren berri izan zutenean, hainbatek bi eta bi batu eta pentsatu zuten agian Intelen txipek ez zutela egiten esaten zutena, NSAk ezagutzen zuen algoritmo bat inplementatu baizik. Hala, NSAk web-zerbitzu gehienen gako pribatuak lortzeko bidea izango zuen Inteli eta hark Linuxen jarritako atzeko ate horri esker. Konspiranoikoegia dirudi, ezta? Hala ere, Linuxen kolaboratzaileetako batzuek utzi egin zioten bertan laguntzeari, eta eskaera bat ere egon zen Change.org-en RdRand Linuxetik erretiratzeko. Baina Linus Torvaldsek, Linuxen asmatzaile eta egungo koordinatzaile nagusiak, gogor erantzun zien, hori ausazkotasun-iturrietako bat besterik ez zela esanez eta arrazoirik gabeko beldurrak zabaltzea leporatuz.

Bestalde, *Der Spiegel* astekariak argitaratu zuen, irailean hori ere, haien arabera Snowdenen paperetan oinarrituta, Visa eta beste kreditu-txartel batzuen bidez egindako transakzio guztietarako sarbidea ere bazuela NSAk. Ezin da jakin hori egia den. Baina ia astero ari dira agertzen horrelako susmo eta teoria berriak.

NOLA BABESTU GURE PRIBATUTASUNA?

Komunikazio digitalen intertzeptazio hori, jakina, segurtasunaren izenean egiten dute. Baina, normalean, okerreko bidean dabilenak neurriak hartzen ditu, eta badaki mezuak eta jarduera sekretupean gordetzen. Eta, azkenean, gobernuek espiatzen dituztenak gu, herritar xumeak, gara. Askok esango du berdin zaiola, ez dela ezer okerrik egiten ari. Baina gure komunikazio digitalak atzitzea pribatutasuna larriki haustea da; mundu analogikoan, gutunak ireki eta irakurtzearen edo telefono-deiak ziztatu eta entzutearen parekoa. Ez genuke horrelakorik onartuko, ezta?

Horregatik, PRISM ezagutarazi zutenetik, eskubide zibilen, askatasunen eta pribatutasunaren aldeko elkarte eta erakundeak haren aurka agertzen ari dira, gizartea kontzientziatu eta mobilizatzen, eta PRISM saihestu eta jendeari pribatutasuna babesteko bideak erakusten. Adibidez, Prism-break.org webguneak bide batzuk erakusten ditu, NSAk gure komunikazio eta datuak atzi ez ditzan. Funtsean, hasieran aipatutako sail honetako artikuluetan ematen genituen jarraibideak segitzean datza (HTTPS erabiltzea, posta GPG edo PGP bidez enkriptatzea, sinadura digitala erabiltzea eta Tor bidez modu anonimoan nabigatzea), eta, horrez gain, PRISM programan dauden enpresen zerbitzu edo softwareen ordez beste aukera batzuk erabiltzea. Softwarearen kasuan, software librea gomendatzen dute beti, iturburu-kodea bistan egotea baita bide bakarra softwareak egiten duenaz ziur egoteko.

Ordenagailuen sistema eragileei dagokienez, Linux da fidagarria den bakarra. Eta, telefonoenei dagokienez, Googlek kontrolatzen ez dituen Androiden aldaerak edo aurreko hilean aipatzen genizuen Firefox OS. iOSek eta Windows Phonek ez dute alternatibarik, iPhoneak eta Windows duten smartphoneak ez erostea gomendatzen dute. Nabigatzeko, Firefox, Tor browser eta beste batzuk daude aukeran (baina ez, Explorer, Chrome, Safari edo Opera). Posta-programa moduan, Thunderbird dugu, eta, webposta nahi izanez gero, MyKolab eta beste zerbitzu batzuk; Gmail, Outlook edo Yahoo! erabiltzekotan, gomendatzen dute Mailvelope Firefoxerako gehigarria erabiltzea (GPG inplementatzen duena). Bilatzaileen artean, aholkatzen dute DuckDuckGo eta beste zerbitzu batzuk erabiltzea ohikoenen ordez, eta, mapei dagokienez, OpenStreetMap. Eta beste zerbitzumota askotarako gomendioak aurkitu ditzakegu webgunean.

Era berean, baina, NSAk saihestu nahi du guk haien atzaparretatik ihes egitea. Lortu dute gure posta-mezuak zuzenean enkriptatuta gordetzen dituzten web-zerbitzu batzuk ixtea, esaterako. Lavabit, Snowdenek erabiltzen zuen zerbitzua, jabeek itxi zuten AEBko gobernuak bezeroen datuak ematera behartu nahi zituelako. Antzeko beste zerbitzu batek, Silent Circle-k, itxi egin du, AEBn zegoenez ez zelako fidatzen zerbitzu erabat segurua eman zezakeenik. Geratzen diren era horretako zerbitzuak AEBtik kanpo daude, Suitzan eta abar.

Badirudi neurri batean behintzat Snowden aferak pribatutasunaren garrantziaz ohartarazteko balio izan duela, eta gorago aipatu ditugun zerbitzu alternatibo, anonimo eta kriptografikoen erabilerak igoera nabaria izan du azken hilabeteotan. Herritarron espioitza digital hau ezagutzeak balio dezala, gutxienez, gure kontzientziak astintzeko, eta, alternatibak bilatzeaz harago, gure zerbitzura egon beharko luketen administrazioek praktika horiek alde batera utz ditzaten behartzen hasteko. ●