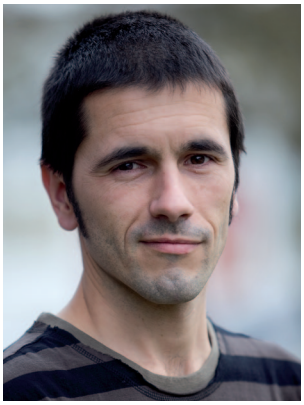

IGOR LETURIA AZKARATE
Informatikaria eta ikertzailea

WEB ENKRIPTATU BATERANTZ?

Edward Snowden AEBko CIA eta NSA agentzietako langile ohiak azaleratu zuenetik gobernuek gure sareko komunikazio eta datuak atzeman eta zelatatzen dituztela, areagotuz joan da sareko pribatutasunarekiko kezka. Eta ez bakarrik erabiltzaileongan: sarearen arduradun eta ingeniariek ere badute kezka hori, eta apurka-apurka web seguruago bateranzko bidea hartu dute.

Sarri izan zen hizpide komunikabideetan Edward Snowden AEBko CIA eta NSA informazio- eta segurtasun-agentzietako langile ohia, hark ezagutarazi baitzituen PRISM eta Tempora programak eta XKeyscore sistema, guztiak segurtasunaren izenean gure sareko komunikazio eta datuak atzemateko eginak.

Horren aurrean, badaude erabiltzaileak har ditzakeen hainbat neurri, webeko segurtasunari buruzko artikuluan kontatzen genizkizuenak. Adibidez, webguneren batean informazio konfidentziala eman behar dugunean (pasahitzak, bankuko kontuak…) HTTPS protokoloa erabiltzen dela ziurtatzea. Badaude nabigatzaileetarako gehigarriak, hala nola HTTPS Everywhere, gure partez arduratuko direnak horretaz. Eta postarako, PGP programa (*Pretty Good Privacy*) edo GPG (*GNU Privacy Guard*) haren bertsio librea erabil ditzakegu; gure mezuak zifratuko dituzte, hartzaileak soilik deszifratzeko moduan.

Alternatiba horiek, baina, beti lan gehigarri bat eskatzen dute instalatzeko eta erabiltzeko, eta kasu batzuetan, gainera, lan hori ez da hain erraza izaten…

WEBAREN OINARRIA SEGURUAGOA EGITEN

Weba seguruagoa izatea ez luke zertan izan erabiltzaileon ardura, ze demontre! Webaren arduradunek egin beharko lukete hori, ezta? Bada, ari dira horretan, neurri bateraino behintzat.

IETF (*Internet Engineering Task Force*) erakundeak, Interneteko protokoloak garatzeko aholkularitza ematen duen erakundeak, badu HTTPBis izeneko lantalde bat, HTTP protokoloaz arduratzen dena. Lantalde horrek HTTP protokoloaren hurrengo bertsioa, HTTP/2, landu eta abenduan aurkeztu zuen estandarraren bertsio berrirako proposamen gisa. Bertsio berri horrek TLS enkriptazioa (HTTPS-k erabiltzen du) beti erabiltzea proposatu zen iazko azaroan, baina polemika sortu zen, eta, adostasunaren mesedetan, azkenean ez dute nahitaezkoa izatea proposatuko. Baina hainbat nabigatzailek esan dute HTTP/2 erabiliko dute soilik TLSrekin batera; bestela, bertsio zaharra erabiliko dutela. Hala, ahal den guztietan behintzat, konexio segurua erabiliko da.

Beste ekimen bat ere izango da 2015ean EFF edo Electronic Frontier Foundation, Mozilla Fundazioa (Firefox nabigatzailearen egilea) eta beste batzuen eskutik: Let's Encrypt. Hau ziurtagiri-jaulkitzaile berri bat izango da, dohainik eta segundo gutxitan HTTPS zerbitzua eskaini ahal izateko ziurtagiri bat emango diguna (2013ko apirileko Interneteko autentifikazioari buruzko artikuluan azaldu genizuen hau zehatzago). Halako erraztasunak emanda, pentsatzekoa da etorkizunean orain baino askoz webgune gehiagok eskainiko dutela HTTPS konexio seguru eta zifratua.

Horrez gain, badago DNS (*Domain Name System*) zerbitzua ere seguruagoa eta konfidentzialagoa egiteko asmoa. DNS zerbitzua arduratzen da

ARG.: PSDESING1/DOLLARPHOTOCLUB

guk webean jartzen dugun domeinu-izen bat (aldizkaria.elhuyar.org, google.com…) Internetek zerbitzari eta ordenagailuak izendatzeko erabiltzen dituen IP zenbaki bihurtzeaz (54.235.134.181, 212.142.160.208...). Baina informazio hori enkriptatu gabe doanez, edonork ikus edo manipula dezake. Orain DNSCrypt protokoloa sortu dute, gure ordenagailuaren eta DNS zerbitzariaren arteko komunikazioak zifratuta joan daitezen. Hainbat DNS zerbitzarik jada inplementatua dute, eta pentsatzekoa da nabigatzaileak ere inplementatuz joango direla.

Bestalde, nahiz eta guk gure posta elektronikoko hornitzailearekiko komunikazioetarako beti HTTPS, SMTPS edo IMAPS protokolo seguruak erabili, mezuak hornitzaile batetik bestera doazela bidean atzeman daitezke. Hori ekiditeko, gero eta posta hornitzaile gehiagok erabiltzen dute TLS zifratua beren arteko mezu-transferentzietan.

Azkenean, poliki bada ere, weba gero eta seguruagoa egiteko ahaleginak egiten ari dira haren arduradunak. Izan ere, webaren espiritua beti izan da irekia eta erabiltzailearen onerakoa, eta weba gidatzen duen erakundeak, W3Ck, eta haren zuzendari eta webaren asmatzaile Tim Berners Leek, beti erakutsi dute estandar irekien, komunikazioen segurtasunaren eta gizartearen ongizatearen aldeko jarrera.

Baina horrek ez du ezertarako balioko erabiltzaileok jarraitzen badugu gailu mugikorretako aplikazioak gero eta gehiago erabiltzen, weba erabili beharrean. Aplikazio horiek enpresek egiten dituzte, interesak dituzten enpresek, eta komunikazioetarako beren protokoloak erabiltzen dituzte; inork ez daki nola dabiltzan protokolo horiek, seguruak diren edo ez... Badakigu zein den mugikorretan mezularitzarako gehien erabiltzen den programa, nahiz eta ezagunak izan haren segurtasun-arazoak…

> *“Poliki bada ere, weba gero eta seguruagoa egiteko ahaleginak egiten ari dira haren arduradunak”*

Konponbidea Internet osatzen duten ordenagailu eta nodo guztien arteko komunikazio guztiak enkriptatuta joatea litzateke. Hala, berdin izango litzateke zein protokolo edo zein aplikazio erabiltzen ari garen, dena enkriptatuta joango litzateke inongo hirugarrenek ezin atzeman izateko moduan. Bada hori ere proposatu du IAB edo Internet Architecture Board erakundeak, Interneten garapen teknikoaz eta ingeniaritzaz arduratzen den erakundeak, hain zuzen: Interneteko komunikazio guztiak behe-mailan zifratzea.

Edonola ere, noizbait webean dabilen komunikazio guztietarako erabateko segurtasuna eta konfidentzialtasuna lortuko balitz ere, horrekin lortuko genuke sarean hirugarrenek ez izatea aukerarik gure komunikazioak atzitzeko. Baina jasotzaileaz ziur egon gaitezke? Snowden-ek ezagutarazitakoaren arabera, PRISM programan, webeko hainbat hornitzailek ematen diote informazio guztia NSAri: Google, Yahoo, Skype, Dropbox… Horiek erabiliz gero, ezin ziur egon gure datuak pribatuak izaten jarraituko duten. Hori lortu nahi izanez gero, aipatu ditugun enkriptazio- eta babes-sistema konplikatuagoak erabiltzea beste aukerarik ez dago...