IGOR LETURIA AZKARATE
*Informatikaria eta ikertzailea*

INTERNETEKO KOMUNIKAZIOEN SEGURTASUNA II

# Autentifikazioa

**Interneteko komunikazioen segurtasunari buruzko aurreko artikuluan ikusi genuen badagoela modua konfidentzialtasuna bermatzeko (guk jasotzaile bati bidalitako mezu edo komunikazio bat hirugarrenek ez atzeman ahal izateko). Hala, hirugarrenek ezin badute mezua atzeman, guri jasotzailea direla sinetsaraztea da informazioa lortzeko modu bat. Hori ekiditeaz arituko gara artikulu honetan, autentifikazioaz hain zuzen ere.**

Mundu errealarekin analogia bat egite aldera, denda edo jatetxe batean txartelaren bidez ordaintzearen kasua har dezakegu kontuan. Aurreko artikuluan ikusi genuena izango litzateke txartelaren datuak eta tekleatzen dugun kodea besteen begiradetatik ezkutatu beharra eta hori egiteko modua; oraingoan, berriz, zerbitzaria, denda edo dena delakoa fidatzekoak direla ziurtatu beharraz eta hori egiteko moduaz arituko gara.

Izan ere, Interneten ere arazo bera dago: on line denda batean erosten ari garela, nola dakigu denda hori berak dioena dela, eta ez dela gure datuak lortzeko benetako dendaren itxura bereko webgunea muntatu duen lapur bat? Hori baita *phishing* delako iruzurra: banku edo denda baten antz handia duen webgune bat egiten da, URLa ere oso antzekoa duena, eta erabiltzaileak bertara erakartzen dira, normalean posta elektronikozko mezu baten bidez; han sartzen ditugun pasahitz edo txartelen datuak iruzurgilearen esku gelditzen dira. Antibirus batzuek badituzte *phishing* detektagailuak, baina ez dira % 100 seguruak. Onena URLa ongi begiratzea da, arrasto susmagarrien bila. Baina beti ez da erraza izaten iruzurrak atzematea. Ba al dago, bada, Interneten mekanismorik webgune bat esaten duena dela bermatzeko, hau da, webgunea autentifikatzeko?

## WEBGUNEEN AUTENTIFIKAZIOA, HTTPS BIDEZ

Aurreko artikuluan aipatutako HTTPS protokoloak bermatzen du hori. Han ikusi genuenez, HTTPS protokoloak gako publiko bidezko kriptografia erabiltzen du, hau da, mezua zifratzen da jasotzailearen gako publikoa erabiliz, baina mezua ezin da deszifratu edozeinek ezagutzen duen gako publiko horren bidez, baizik eta jasotzaileak soilik ezagutzen duen gako pribatuaren bidez; horrela bermatzen da jasotzaileak soilik irakurriko duela gure mezua. Horrek, berez, ziurtatzen du gure datuak enkriptatuko direla eta ezingo dituela beste inork atzeman. Baina autentifikazioa HTTPS protokoloaren beste ezaugarri bati esker bermatzen da: gako publikoaren ziurtagiri digitalak.

Ziurtagiri digitalak entitate digital baten eta haren gako publikoaren arteko lotura bermatzen duten dokumentu digitalak dira, hirugarren pertsona fidagarri batzuek (ziurtagiri-jaulkitzaileek) jaulkitakoak. Hala, on line dendek HTTPS zerbitzari bat martxan jartzeko ziurtagiri bat lortu behar dute aurretik jaulkitzaile batekin (edo gehiagorekin). Eta nabigatzaile batek HTTPS konexio bat hasi behar duenean, egiten duen lehenengo gauza da ziurtagiri jaulkitzaileekin konektatu eta webgune horren ziurtagiri digitala eskatu, ziurtatzeko benetan esaten duen enpresarena dela eta gako publikoa zuzena dela.

Ziurtagiri digitalarekin dena ongi badago, ziurtagiriaren datuak ikus ditzakegu helbide-barran agertzen den giltzarrapoaren ikonoan klik eginda. Hala ez bada, ziurrenik behin baino gehiagotan ikusiko zenuen ohar bat erakusten digu nabigatzaileak, polizia bat dokumentazioa eskatzen agertzen den ikono batekin. Hori agertzen den guztietan ez du esan nahi iruzurrezko webgune baten aurrean gaudenik: baliteke gure nabigatzaileak ez izatea ziurtagiri-jaulkitzaile horren berri (zaharkitua dagoelako, esaterako), edo webgunea talde murriztu batentzat soilik izatea (enpresa bateko estraneta, adibidez) eta ziurtagiririk ez eskatu izana; ziur bagaude webgunea segurua dela, aurrera egiteko aukera ere ematen digu nabigatzaileak.

Beraz, datu pribaturen bat (pasahitz bat, dokumentu konfidentzial bat, kreditu-txartelaren datuak...) sartu behar badugu webguneren batean, HTTPS protokoloari dagokion giltzarrapoa ikusten badugu eta nabigatzaileak ez badigu oharrik egiten, lasai egin dezakegu, ziur egon baikaitezke jasotzailea esaten duena dela eta beste inork ezingo duela atzeman.

ARG.: © BRUCE ROLFF/123RF

*“Iruzurra egiteko bide bat posta elektronikoa da. Sinadura digitalaren bidez jakin dezakegu gure solaskidea berak dioena dela”*

## POSTA-MEZUA BIDALTZEN DUENAREN AUTENTIFIKAZIOA

Iruzurrak egiteko beste bide bat posta elektronikoa da. Ezagutzen dugun norbaiten izenean mezu bat irits dakiguke informazio bat eskatuz edo jarraibide batzuk emanez, eta dioena eginez gero datuak lapurtu diezazkigukete; izan ere, erraza da posta elektronikozko mezu bat beste norbaiten izenean bidaltzea. Ba al dago modurik, beraz, bidaltzailea autentifikatzeko? Bai, sinadura digitalaren bidez.

Sinadura digitala, funtsean, gako publiko bidezko kriptografiaren erabilera berezi bat da. Bidaltzaileak mezuaren kopia bat gako pribatua erabiliz enkriptatzen du eta jasotzaileak, desenkriptatzeko, bidaltzailearen gako publikoa erabiliko du, ziurtagiri-jaulkitzaile batengandik lortua; desenkriptatutakoa jatorrizko mezuaren berdina bada, horrek esan nahi du mezua ustezko bidaltzaileak bidalitakoa dela nahitaez, berak soilik baitu haren gako pribatua.

Posta elektronikoko programek (Outlook, Thunderbird...) izaten dute mezuak digitalki sinatzeko aukera, batzuek berezkoa eta beste batzuek PGP programa (Pretty Good Privacy) edo GPG (GNU Privacy Guard) haren bertsio librea instalatuta. Halako programei buruz ere aurreko artikuluan hitz egin genizuen, esanez gako publiko bidezko kriptografia erabiltzen dutela mezua enkriptatzeko eta jasotzaileak soilik desenkriptatu ahal izateko. Baina ez da hori halako programek egiten duten gauza bakarra: sinadura digitala ere inplementatzen dute bidaltzailea autentifikatzeko. Web bidezko postarekin (Gmail, Hotmail, Yahoo...), aldiz, ez da aukerarik digitalki sinatzeko. Izan ere, horrek eskatuko luke gure gako pribatua hornitzailearen esku uztea, eta hori ezin da egin, gako publiko bidezko kriptografia fidagarria izateko gako pribatua norberak soilik gorde behar baitu. Aukera bakarra izan daiteke nabigatzailearentzako plugin bat erabiltzea, enkriptazioa norberaren ordenagailuan egingo duena.

Laburtuz, nabigatzean HTTPS protokoloa darabilten webguneetan ibilita eta postan PGP, GPG edo beste moduren baten bidezko sinadura digitala erabilita, ziur egon gaitezke ez soilik datuak beste inork ez dituela atzemango, baizik eta baita gure solaskidea berak dioena dela ere.●