IGOR LETURIA AZKARATE
Informatikaria eta ikertzailea

Gaur egunean informazio oso garrantzitsua ibiltzen da Interneten zehar: posta elektroniko pribatuak, dokumentu konfidentzialak, online zerbitzuetako kontuen pasahitzak, kreditu-txartelen datuak... Baina seguru al doa informazio hori guztia Internetetik?

INTERNETEKO KOMUNIKAZIOEN SEGURTASUNA I

Konfidentzialtasuna

E-mailean, webean nabigatzen, nahiz Interneten beste zerbaitetan ari garela, informazioa bidaltzen dugu; abiapuntutik helburura iristeko informazio hori puntu askotatik pasatzen da: gure ordenagailu edo bestelako gailu digitaletik ateratzen da, bideragailuren batetik pasatuko da (enpresako sareko routerretik, etxeko edo tabernako wifikotik...), gero Internet-hornitzailearengana iritsiko da, eta handik oraindik beste nodo asko pasatuko ditu helmugara iritsi arte. Tarteko puntu horietako edozeinen kontrola duenak, dela enpresako informatikaria, tabernako jabea edo Interneteko hornitzailearekin elkar hartuta dagoen polizia —edo, wifiaren kasuan, baita wifidun ordenagailu bat hurbil duen edozeinek ere—, erraz atzeman dezake informazioa.

Sareko komunikazioen zati handi bat (webeko nabigazio gehiena, posta-jasotze eta -bidaltze asko) irekian doa, edozeinek atzemateko moduan. Baina Internetek baditu mekanismoak informazio sentibera —adibidez, pasahitzak, kreditu txartelen datuak edo posta elektroniko sekretuak— modu seguruan eta konfidentzialtasuna bermatuz garraiatzeko. Kriptografiaz baliatzen da horretarako, hau da, mezuak enkriptatuz (kodetuz edo zifratuz) jasotzailea ez den edozeinentzat ulertezin bihurtzen dira. Zehazki, kriptografia-mota berezi bat erabiltzen da Interneten: gako publiko bidezko kriptografia edo kriptografia asimetrikoa.

KRIPTOGRAFIA KLASIKOAREN ARAZOAK INTERNETEN

Mezuak enkriptatzeko sistemak asko erabili izan dira historian zehar, batez ere errege, jeneral eta bestelako agintarien arteko komunikazio garrantzitsuetarako, baina baita maitaleen arteko amodio-mezu sekretuentzat ere. Hasieran metodo sinpleak zirenak gero eta konplexuago bihurtu dira, teknologiak horretarako bidea eman ahala eta aurreko sistemak hausteko teknikak aurkitu ahala. Historiako enkriptatze-metodo ezagun eta erabilienen artean, aipa genitzake Zesarren zifra, Vigènere-ren zifra eta errotore-makinak (Lorenz-ena eta Enigma, esaterako).

Funtsean, enkriptazio-sistema horiek denak printzipio berean oinarritzen dira: mezua funtzio baten bidez eraldatzen da, gako bat erabiliz, eta jasotzaileak gero alderantzizko funtzioa aplikatzen du gako berarekin jatorrizko mezua lortzeko. Adibiderik sinpleenean, funtzioa kenketa izan daiteke eta gakoa 1 zenbakia. Hala, "IBM" mezua "HAL" bihurtuko litzateke letra bakoitzari "-1" funtzioa aplikatuz aurreko letrarekin ordezten badugu, eta jasotzaileak, gakoa (1 zenbakia) jakinda mezu zifratuari "+1" funtzioa aplikatuta, "IBM" lortuko luke berriro. Honi kriptografia simetriko deitzen zaio, gako bera erabiltzen duelako enkriptatzeko eta desenkriptatzeko.

> *"Gako bat beste inork jakin ez dezan, ezin da Internetez bidali, atzeman egin baitaiteke"*

Sistema hauek gero eta hauskaitzago bihurtu dira, zifratze-funtzioa gero eta konplikatuago egin dutelako, garai bakoitzeko teknologiaren laguntzarekin. Gaur egun, kriptografia egiteko ordenagailuak erabiltzen dira; haiei esker, aipatutako funtzioak oso konplexuak eta gakoak oso luzeak izan daitezke, sistema erabat hautsezinak garatzeko modukoak. Hala, AEBko Gobernuak (beste askoren artean) erabiltzen duen AES (*Advanced Encryption Standard*) zifraketa, kriptografia simetrikoko sistema da.

Baina horrelako sistemek arazo bat dute Interneten jende guztiak nabigatzeko, online erosteko edo e-mail pribatuak bidaltzeko erabiltzeko orduan: bi aldeek ezagutu behar dute gakoa eta beste inork ez. Beraz, ezin da beti gako bera erabili, gako ezberdin bat behar da jasotzaile eta bidaltzaile bakoitzeko; eta gako hori beste inork jakin ez dezan, ezin da Internet bidez bidali, jakina, lehen esan bezala, atzeman egin baitaiteke. Horiek horrela, kasu batzuetan, gobernuenetan esaterako, mezulari bidez bidal

ARG.: © SERGEY NIVENS/123RF

dakioke gakoa komunikatu nahi den erakunde bakoitzari, baina Interneteko komunikazioentzat? Denda eta bezero bakoitzeko, webgune eta bisitari bakoitzeko, posta elektronikoaren bidaltzaile eta jasotzaile bakoitzeko, lehenago gako bat aurrez aurre partekatu behar izatea edo mezulari bidez bidali behar izatea ezinezkoa da praktikan: oso garestia litzateke eta ez segurua gainera (mezulariak ustelduta egon daitezke edo gakoa lapurtu egin diezagukete bidean).

GAKO PUBLIKO BIDEZKO KRIPTOGRAFIA

Merkataritza elektronikoak eta Internet bidez informazio konprometitua bidaltzeak aurrera egin badu, 1970eko hamarkadan zifratze-sistema berri bat asmatu zelako izan da, ordura arteko sistemen aldean erabat ezberdin eta apurtzailea, intuizioaren guztiz aurkakoa eta aldi berean oso segurua: gako publiko bidezko kriptografia edo kriptografia asimetrikoa.

Gako publiko bidezko kriptografian, zifratzeko funtzio bat eta gako bat erabiltzen dira, baina funtzio horrek ez du alderantzizkorik (noranzko bakarreko funtzio deitzen zaie hauei); beraz, gakoa jakinda ere ezin da mezua deszifratu; deszifratzeko beste funtzio bat eta beste gako bat behar dira (horregatik deritzo kriptografia asimetrikoa). Orduan, norbaitek ahalbidetu nahi badie beste batzuei modu pribatuan berarekin komunikatzea (esaterako, saltzaileak erosleei, haiek kreditu-txartelaren datuak bidali ahal izateko), publiko egiten du enkriptatzeko gakoa. Edozeinek erabili ahal izango du gako publiko hori hari mezu zifratu bat bidaltzeko, baina gako publiko hori mundu guztiak ezagututa ere, mezua hark bakarrik deszifratu dezake, hark bakarrik ezagutzen baitu deszifratzeko gakoa (gako pribatua deritzona).

Sistema honek funtziona dezan, beharrezkoa da existitzea gako baten araberako funtzio bat alderantzizkorik ez duena, alderantzikatzea beste funtzio eta beste gako baten bidez lortzen dena, eta bigarren gakoa lehenengoa jakinda kalkulatu ezin daitekeena. Guztiz intuizioaren aurkakoa da horrelako funtzio eta gako batzuen existentzia, baina izan badaude, aritmetika modularrari, zenbaki lehenei eta faktorizazioari esker. Ron Rivest, Adi Shamir eta Leonard Adleman MIT (Massachusetts Institute of Technology) entzutetsuko ikertzaileek aurkitu zituzten horrelako lehenengoak 1977an.

Esan dugu sistemak funtzionatzeko baldintzetako bat dela deszifratzeko gakoa ezin kalkulatu ahal izatea zifratzeko gakotik abiatuta. Baina, logikoa denez, biak erlazionatuta daude eta kalkulatu daiteke bigarrena lehenetik abiatuta: faktorizazioa egitea besterik ez da, hau da, zenbaki horren zatitzaileak ateratzea. Kontua da hori egin ahal izateko ez dagoela formula azkarrik; zenbaki guztiak probatuta besterik ezin da egin momentuz. Beraz, zenbaki horiek nahikoa handiak badira (eta ehunka digitukoak erabiltzen dira), gaur egungo teknologiarekin ezinezko problema bihurtzen da faktorizazioa, eta

"Gako publiko bidezko kriptografian, gakoa jakinda ere ezin da mezua deszifratu; beste funtzio bat eta beste gako bat behar dira"

zifratze-sistema hautsezina da praktikan. RSA izena du metodoak, asmatzaileen omenez; nahiz eta geroago jakin zen metodo hori Clifford Cocks GCHQ (Government Communications Headquarters, edo Britainia Handiko Inteligentzia Zerbitzua) erakundeko langileak asmatu zuela 1973an, hau da, lau urte lehenago, baina erakunde horren informazio guztia sekretua zen eta 1997ra arte ez zen hori jakinarazi.

RSAren ondoren asmatu dira gako publiko bidezko beste kriptografia-sistema batzuk, hala nola DSA edo ElGamal.

KONFIDENTZIALTASUNA INTERNETEN

Interneteko komunikazioak OSI ereduaren arabera mailatan antolatuta daude, aurreko zenbakian kontatzen genizuenez. Eta komunikazio horien konfidentzialtasuna bermatzeko, garraio-mailarako TLS protokoloa (*Transport Layer Security*) definitu da (lehen SSL edo *Secure Sockets Layer* gisa ezagutzen zena). Honetan, bidaltzaileak eta jasotzaileak gako publiko bidezko kriptografia erabiltzen dute (RSA normalean, baina besteren bat izan daiteke, biek inplementatuta badute) beste gako bat adosteko (ausazkoa), eta gero benetako komunikazioa gako horrekin eta kriptografia simetriko bidezko metodo batekin egiten da (AESekin, adibidez), konputazionalki ez delako hain garestia eta segurtasun parekoa eskaintzen duelako.

Interneteko aplikazio-mailako protokolo bakoitzerako (weberako HTTP, postarako SMTP eta IMAP, fitxategiak igotzeko FTP, urruneko ordenagailuetan saioak irekitzeko Telnet...), haien bertsio seguruak sortu dira (HTTPS, SMTPS, IMAPS, SFTP eta SSH hurrenez hurren). Horietako batzuk, adibidez HTTPS, SMTPS edo IMAPS, jatorrizko protokoloari garraio-mailan TLS gehitzean eta protokolo berriari beste portu bat esleitzean besterik ez dautza (orain, STARTTLS protokolo berriaren bidez, aplikazioek portu bera erabili dezakete konexio seguruentzat, alde biek inplementatuta duten kasuetan). Beste batzuk, SFTP eta SSH kasu, funtzio berdina dute baina protokolo ezberdinak dira, gako publiko bidezko enkriptazioa erabiltzen dutenak. Protokolo horiek erabiltzen direnean, gure komunikazioen konfidentzialtasuna bermatutzat jo dezakegu. Eta nola jakin protokolo horiek erabiltzen ari garen?

Webean nabigatzen ari garenean, helbidean giltzarrapo bat eta beronen hasieran "https://" ikusten badugu, esan nahi du HTTPS protokoloa erabiltzen ari garela eta, beraz, komunikazioa segurua dela. Merkataritza elektronikoko guneetan ordaintzean, web bidezko posta bezalako zerbitzuetan eta beste toki askotan normalean erabiltzen da.

Merkataritza elektronikoko guneetan, web bidezko posta-zerbitzuetan eta beste toki askotan ohikoa da HTTP-aren bertsio segurua: HTTPS.
ARG.: © VLAD KOCHELAEVSKIY/123RF

Posta-programen kasuan, gure kontuaren ezarpenetan begiratu beharko dugu ea zein protokolo onartzen dituen posta bidali eta jasotzeko. Edonola ere, nahiz eta posta programak SMTPS eta IMAPS protokoloak erabili, esan nahi du gu eta gure posta-hornitzailearen arteko komunikazioa inork ezingo duela irakurri, baina ez bidalketaren ondorengo faseetan beste inork ez duenik irakurriko. Hori ekiditea nahi badugu, gure posta-programan PGP programa (*Pretty Good Privacy*) integratu dezakegu (Phil Zimmermannek 1991n sortua eta oso ezagun eta erabilia bihurtu dena) edo GPG (*GNU Privacy Guard*) haren bertsio librea; biek azken hartzailearen gako publikoa erabiliz zifratzen dute informazioa, eta, beraz, hark baino ezingo du irakurri.

Urruneko ordenagailuetan saioak irekitzeko edo fitxategiak igotzeko, SSH edo SFTP protokoloak erabiltzen direla ziurtatu beharko dugu konfidentzialtasuna mantendu nahi badugu. Bestelako programetan (VNC, VPN edo Sare Pribatu Birtualak...), ezarpenetan begiratu beharko dugu ea enkriptaziodun protokoloak edo enkriptazio-sistemak erabiltzen dituzten. Gauza hauek kontuan izanez gero, gure informazio pribatuak hala izaten jarraituko du Internet bidez bidalita ere. ●

"Protokolo seguruak erabiltzen direnean, gure komunikazioen konfidentzialtasuna bermatutzat jo dezakegu"

Segurtasunaren, konfidentzialtasunaren eta kriptografiaren gaia interesatzen bazaizu, informazio gehiago aurkituko duzu Elhuyar Fundazioak euskaraz argitaratu duen Simon Singh-en Kodeen liburua *interesgarrian.*