Liher Elgezabal: "kriptografia alde batetik artea eta bestetik zientzia da"

Eneko Imaz Amiano
Elhuyar

Ordenagailuen erabilera hedatu eta mezuak sare bidez bidaltzea arrunt bilakatzen hasi zenean, askok mezuak seguru bidaltzeko modua zelako sentsazioa sentitu zuen. Baina gu sarean egon bagaitezke, gainerakoak ere egon daitezke, eta, mezuak sarean zehar pasatzen badira, inork 'harrapatu' ere egin ditzake, telefonoa kontrolatzen den bezalaxe. Horren aurrean babesteko modua kriptografia erabiltzea da. Eta horretan aditua da gure zenbaki honetako gonbidatua.

E. IMAZ AMIANO

Liher Elgezabal 25 urteko bilbotarra dugu. Informatikaria da eta, gaur egun, informatikako ingeniari tekniko izateko ikasketak egiten ari da UNEDen. Aldi berean, Micromuse garapen-enpresan lan egiten du, Londresen. Aurretik, Ingeniari Tekniko Industrialen Elkargoan sistema-administratzaile izan zen eta SICE enpresan bideo bidezko segurtasun-sistema informatizatu bateko administratzaile-lanetan aritu zen. Kriptografiari buruzko hitzaldia eman du aurten UEUn.

Kaixo Liher, Londresen ari zara lanean. Nolatan?

Londresera etortzeko arrazoi nagusia jakin-mina izan zen. Linux-en eta software librearen oso zalea naiz eta, garai hartan era horretako softwarearen erabilpena nahiko mugatua zenez, atzerrira etortzea erabaki nuen. Geroztik, Londresen eta New Yorken izan naiz lanean eta hainbat ikasteko aukera izan dut.

Zer da Micromuse enpresan egiten duzuena? Eta zer da zehazki zuk egiten duzuna?

Micromusek software-garapena egiten du. Datu-sareen segurtasuna denbora errealean monitorizatzeko aplikazioak egiten ditugu, eta telekomunikazio-enpresa handiek sare erraldoiak kontrolatzeko erabiltzen dituzte.

Nik softwarearen kalitatea kontrolatzeko departamentuan lan egiten dut, gure programen programazio- eta segurtasun--akatsak bilatzen. Hori automatikoki egingo duen akats--bilatzaile bat garatzen dihardut.

Kriptografiaren gaiari helduz, ordenagailuz egiten diren komunikazioen segurtasun-sentsazio hori faltsua da, ezta? Erraza al da sarean dabiltzan mezuak atzematea?

Zoritxarrez, gaur egun segurtasuna erabiltzaileon eskuetan dago erabat, Internetek ez baitu inolako segurtasunik eskaintzen.

Posta arruntean, mezua kartazalik gabe bidaliz gero, postariak mezuak irakurtzeko aukera izango du. Gauza bera gertatzen da posta elektronikoaz.

Sareen hedapenak asko erraztu du komunikazioa, baina ez dugu sarearen, hau da, komunikazio-kanalaren batere kontrolik.

Ohikoa al da mezuak atzematea? Zein izaten dira arrazoi nagusiak?

Idazkera existitzen denetik, mezu idatziak atzematen saiatu da gizakia. Arrazoiak oso ezberdinak izan daitezke, jakin-min hutsetik hasi eta arrazoi ekonomiko, politiko edo militarrak barne. Informazioa beti izan da baliabide oso preziatua.

Egungo komunikazio gehienak era digitalean transmititzen eta biltegiratzen dira, eta horrek asko errazten ditu datuen atzemate, kopiatze, iragazte eta bestelako prozesaketa automatizatuak.

"gaur egun, segurtasuna erabiltzaileon eskuetan dago erabat, Internetek ez baitu inolako segurtasunik eskaintzen"

Gure informazio pertsonala, historial klinikoa, bankuko mugimenduak, telefono-deien zerrenda eta abar, era digitalean biltegiraturik daude, eta informazio hori gehienetan sarean zehar sakabanatuta dago. Horrek informazioa behar bezala babesteko beharra nabarmentzen du.

Pentsa daiteke norbera erabiltzaile arrunta izanik, inor ez dela bere mezuak atzematen ibiliko, edo atzemanez gero ere berdin zaiola.

Nahiz eta gure informazioaren balioa txikia izan, oso arraroa da gutun bat kartazalik gabe bidaltzea. Behatuak sentituko ginateke, gutunak hainbat bitartekoren eskuetatik pasa behar duela ohartzen baikara. Pertsona batek makina batek baino mesfidantza handiagoa sortarazten digu, baina gogoan izan behar dugu makina guztien atzean pertsonak daudela beti.

Pribatutasuna legez babestutako eskubide bat da herrialde gehienetan. Hala ere, legeok sortzen dituzten erakundeak dira eskubide horri eraso gehien egiten diotenak. Legeak babesten ez bagaitu, matematikaz babestu beharko dugu geure burua.

Eta zure mezuak hartzaile jakin batek, eta ez beste inork, irakurtzea nahi izanez gero, kriptografiara jo behar al da derrigor?

Berez bai; kanala segurua ez den bitartean, mezua nolabait babestu beharko dugu, eta horretarako bidea kriptografia erabiltzea da. Izatez, betidanik egin izan den zerbait da.

Julio Zesarrek bere mezuak kode jakin batez gordetzen zituen etsaientzat ulergaitz bihurtzeko. Era berean, La Celestinaren idazleak bere nortasuna liburuko lerro artean ezkutatu zuen bere burua babesteko.

Gaur egun, ordenagailuen ahalmenari esker, funtzio matematiko konplexuak erabiltzen dira mezuak zifratu eta ezkutatzeko.

Zer da kriptografia? Zertan datza?

Kriptografia alde batetik artea eta bestetik zientzia da. Helburua testuak, soinuak, irudiak edo beste edozein eratako informazioa ulergaitz bihurtzea da.

Kriptografiaren oinarria jatorrizko testuaren gainean eraldaketak gauzatzean datza, hizkien kokapena aldatuz (lekualdatzea) edo hizkiak ordezkatuz (ordezkatzea). Adibidez:

elhuyar --- (binaka trukatuz) ---> leuhayr
elhuyar --- (alfabetoan + 3) ---> hñkybdu

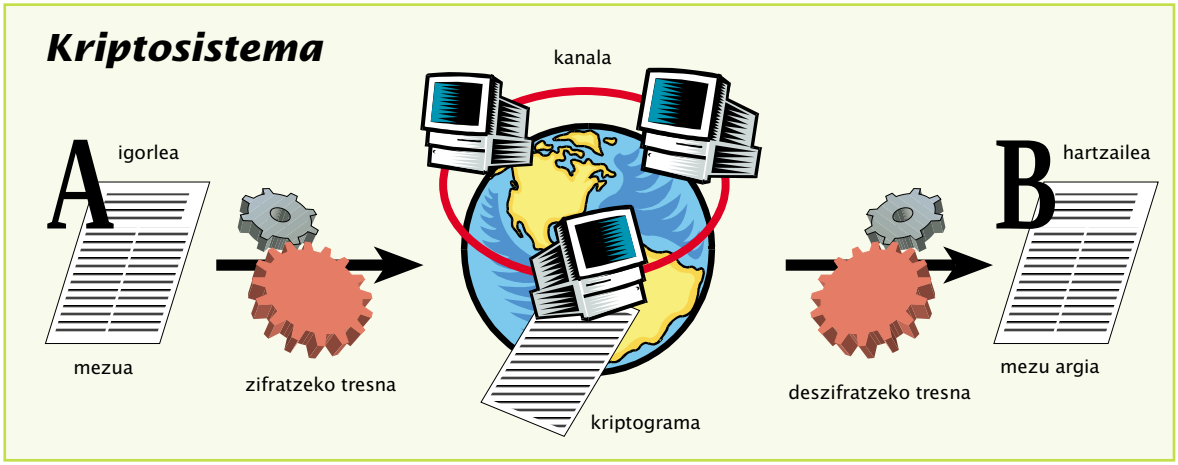
Kriptografia-algoritmo batek eraldaketa hauek nola gauzatzen diren definitzen du. Gaur egun erabiltzen diren algoritmoak publikoak eta ezagunak dira. Algoritmo hauek aldagai baten arabera informazioa era batean edo bestean eraldatuko dute. Aldagai honi gakoa deritzo. Kriptosistemaren segurtasuna gakoan datza, ez algoritmoan bertan.

Mezuak zifratzeko sistema bakarra al dago? Zer desberdintasun dago sistemen artean?

Aipatu bezala, gure mezuak zifratzeko gako bat behar dugu eta gakoa sekretupean gorde. Gako honen arabera, kriptografia-sistema ezberdin bi bereizten dira.

Kriptografia simetrikoak gako bera erabiltzen du mezua zifratzeko eta deszifratzeko.

Demagun segurtasun-kutxa bat dugula eta bertan gure sekretuak gorde nahi ditugula. Sarraila 3 digituko konbinaketa baten bidez ixten da. Ixteko 0-7-4 konbinaketa erabili badugu, zabaltzeko konbinaketa bera erabili beharko dugu.



Kriptografia asimetrikoa, aldiz, gako osagarriez baliatzen da mezuak zifratu eta deszifratzeko. Gako batek zifratzen duena beste batek bakarrik deszifra dezake, eta alderantziz.

Demagun segurtasun-kutxa diseinatzean bi gakoen baturak, 8-0-0 izan behar duela finkatu dugula eta datu hau guk geuk bakarrik ezagutzen dugula. Segurtasun-kutxa ixteko 2-0-0 konbinaketa erabili baldin badugu, zabaltzeko 6-0-0 konbinaketa erabili beharko dugu.

Sistema hau erabiliz, zifratze-gakoa (2-0-0 kasu honetan) publiko egin daiteke, deszifratzeko ez baitu balio. Mezua edozeinek zifra dezake, baina geuk bakarrik deszifratu ahal izango dugu. Gako bat jakinez gero, ez da posible beste gakoa kalkulatzea, bien batura (8-0-0) ezezaguna baita.

Zifratzeko programak ere bat baino gehiago izango dira. Guztiek gauza bererako balio al dute?

Adibiderik ezagunena PGP (Pretty Good Privacy) delako programa librea da. Posta elektroniko segurua erabiltzeko diseinatu zen, nahiz eta beste erabilpen batzuk ere onartzen dituen. PGPri esker, ordura arte gobernu edo erakunde militarren esku besterik ez zegoen kriptografia sendoa erabiltzaile arruntengana hurbiltzea lortu da.

> *"hala ere, nire ustean denetan zailena ingurukoei kriptografia zer den eta zergatik erabili behar duten azaltzea da"*

Gero eta gehiago erabiltzen dugun beste inplementazio bat X.509 deritzona da. Nabigatzailerik ezagunenek estandar hau integratuta dakarte, eta komertzio elektronikoa era seguruan bideratzeko erabiltzen da.

Mezuak babestea al da kriptografiaren helburu bakarra?

Ez, inolaz ere. Mezua ezkutatzea erabilera posible bat da, baina kriptografiak beste hainbat aplikazio ditu. Besteak beste, mezuaren osotasuna ziurtatzeko edo mezuaren idazlearen nortasuna egiaztatzeko aukera ematen du. Azkeneko bi hauek dira, hain zuzen, sinadura digitalaren oinarri.

Mezuak baimenik gabe atzeman eta irakurtzeko sistemak ere egongo dira, noski.

Kriptoanalisiak kriptograma bat baimenik gabe irakurtzeko bideak aztertzen ditu.

Hizkuntza bakoitzak hizki-errepikapen ezberdin batzuk jarraitzen ditu. Era berean, hizkuntza bakoitzean hizki batzuek zenbat aldiz agertzen diren azter daiteke. Informazio hau kontuan izanik, kriptograman % X aldiz agertzen den Y hizkia jatorriz zein hizki izan daitekeen suposa liteke.

ARTXIBOKOA

Amaitze aldera, ba al dago kriptosistema erabat segururik?

Kriptografiak sekretu handi bat (gure mezua) sekretu txiki batez (gakoa) babesten du. Eta gaur egungo kriptografia-sistemen sendotasuna gakoaren luzeran oinarritzen da.

Segurtasun-kutxarekin gertatzen zen bezala, 3 digitu erabiliz gero 1.000 gako ezberdin besterik ez daude; beraz, ustezko erasotzaileak ez du denbora asko beharko kutxa irekitzeko hainbat saiakera eginez.

Gako posible guztiak probatzea posible denez, ez dago benetako kriptosistema segururik. Baina kriptograma bat deszifratzeko beharrezkoa den denbora edo kostua informazioaren balioa bera baino handiagoa baldin bada, kriptosistema sendoa dela esan dezakegu.

Ordenagailu batek, segundoko milioi bat saiakera eginez ere, mila urtetik gora beharko ditu 56 biteko gako posible guztiak frogatzeko. Argi dago ordurako informazioak balioa galdu eingo duela.

Gakoekin eta kriptografiekin ibiltzea ez al da deseroso samarra? Erabiltzaileari lan handia eskatzen al dio?

Mezuak zifratzea eta deszifratzea berehalakoa da PGP programarekin. Hala ere, mezuak zifratzen hasi aurretik, programa instalatu, gako parea (publikoa eta pribatua) sortu, eta gako publikoa banatu beharko dugu. Lan hau ez da bereziki konplikatua. Hala ere, nire ustetan denetan zailena ingurukoei kriptografia zer den eta zergatik erabili behar duten azaltzea da.

Eta zuri dagokizunez, Londresen geratzeko asmoa duzu. Euskal Herrian zuk lan egiten duzun esparruan jarduteko modurik ez al dago?

Egia esan, gaur egun informatika-munduan distantzia hitzak ere zentzua galdu du. Ni Londresen nagoen arren, New Yorken dauden ordenagailuetan egiten dut lan, sarearen bidez.

Euskal Herrian teknologia berria oso azkar sartzen ari da eta teknikari prestatuen beharra ere gero eta nabarmenagoa da. Nik ere egunen batean etxera itzultzeko asmoa daukat, baina oraingoz hemen gustura nago eta hainbat geratzen zait ikasteko eta ikusteko.