WPA3 protokoloa

WiFiak behar zuen eguneraketa

WiFi sareen segurtasuna bermatzen duen WPA protokoloaren bertsio berria, WPA3 izenekoa, atera zuen WiFi Alliancek —WiFi teknologia definitu eta sustatzen duen erakundeak— ekainaren amaieran. Izan ere, aurreko bertsioak, WPA2ak, hamar urte baino gehiago zituen, eta 2017an haustea lortu zuten. Horrez gain, bertsio berri hau prestatuago dago Gauzen Internet hedatzeak ekarriko dituen erronka eta arriskuentzat ere. Sortzaileak oso ziur agertu dira WPA3aren segurtasunaz eta hautsezintasunaz, baina denborak esango du. Edonola ere, denbora apur bat beharko da oraindik WPA3a router eta gailuetan hedatuta ikusteko.

Jende gutxi egongo da gaur egun WiFi teknologia ezagutzen ez duenik, eta are gutxiago, erabiltzen ez duenik. WiFi teknologia erabiltzen da gehien gailuen artean irismen hurbilean haririk gabeko sare lokalak osatzeko. Router deitzen den sarbide-puntu baten bitartez eta WiFi teknologia baliatuta, enpresako edo etxeko sare lokalera konekta daitezke ordenagailu eramangarriak eta telefono mugikorrak, haren Interneteko konexioa erabili eta abar.

WiFi teknologiaren segurtasun-arazoak

Esan bezala, WiFi teknologiak haririk gabeko konexioak ahalbidetzen ditu, airean zehar transmititzen diren uhin elektromagnetikoak erabiliz. Baina horrek esan nahi du segurtasunaren aldetik ahulagoa ere badela. Izan ere, ordenagailu-sare pribatu batean sartzen saiatzeko ez da behar sare hori dagoen eraikinean sartzea eta sare horretara fisikoki kable baten bidez konektatzea, nahikoa da WiFiaren sarbide-puntuaren irismenean egotea, horrela seinale elektromagnetiko guztiak atzeman baitaitezke, sarbide-puntuarekin elkarreragin, eta abar. Horregatik, segurtasuna bermatzeko eta nahi ez diren sartzeak eragozteko, derrigorrezkoa da sistema eta protokolo eraginkorrak izatea.

Igor Leturia Azkarate
Informatikaria eta ikertzailea

WiFi teknologiak erabiltzen duen komunikazio-protokoloa IEEE erakundearen 802.11 protokoloa da, 1997an sortu eta geroztik berritzen joan dena. Lehen bertsio hartan, WEP (*Wired Equivalent Privacy* edo Kable Bidezkoaren Adinako Pribatutasuna) segurtasun-protokoloa barnean zekarren 802.11 protokoloak. Baina segurtasun-sistema horrek laster utzi zion segurtasunezkoa izateari. 2001ean, aircrack-ng softwarea atera zen, zeina gai baitzen WEP baten bidez babestutako WiFi sare baten pasahitza minutu gutxi batzuetan asmatzeko.

IEEE erakundea beste gauza askotan ere aritzen zenez, hainbat komunikazio- eta teknologia- enpresa elkartu, eta haririk gabeko komunikazio-protokoloez berariaz arduratuko zen erakunde bat sortu zuten, 1999an. Erakundeak WECA izena hartu zuen, eta, 2002an, Wi-Fi Alliance gisa birsortu zen. Bera da WiFi izenaren jabea, eta bera arduratzen da WiFi teknologia definitu, sustatu eta ziurtagiriak jaulkitzeaz, eta WiFi teknologiarentzat segurtasun-sistemak sortzeaz.

WiFi Alliancek WPA (Wi-Fi Protected Access) izeneko protokoloa argitaratu zuen, 2003an. Nahiko presaka eta behin-behineko neurri gisa atera zuten, WEP hautsita zegoelako ordurako. Eta, 2004an, WPA2 atera zuen, geroztik WiFi sareetan estandar gisa erabili den segurtasun-protokoloa.

WPA2 sistema ona dela ikusi da, ez baitzaio segurtasun-zulo larririk aurkitu, eta sortu zenetik pasatu diren urte horiek asko dira teknologiaren eskalan. Hala ere, ez da sistema perfektua, eta hainbat akats aurkitu izan zaizkio. Adibidez, erabiltzaileak jarritako pasahitza laburra edo ahula bada, nahiko erraz aurkitu daiteke lehen aipatutako aircrack-ng softwarea erabilita. Bestalde, pasahitza jakinez

gero, deszifratu egin daitezke aurretik eta ondoren pasahitz horrekin zifratuta bidalitako mezu guztiak; horrek esan nahi du edonork ikus ditzakeela mezuak kafetegi, hotel eta halako leku publikoetan (non erabiltzaile guztiek dakiten pasahitza). Horrez gain, frogatu dute WPS sistema ere akastuna dela pantailarik gabeko gailu txikiak (Gauzen Interneteko modukoak) konektatu ahal izateko.

> *"WPA3aren egileak oso ziur eta harro agertu dira haren segurtasunaz"*

Tira, eta WPA2ari ez zaio segurtasun-zulo larririk aurkitu... iaz arte. 2017ko urrian, ikertzaile batzuek argitaratu zuten arazo larri bat aurkitu ziotela, eta frogatzeko, KRACK izeneko erasoa sortu zutela. Horren bitartez, erasotzaile batek pasahitza lortu eta komunikazio guztiak irakurri, deszifratu eta manipula zitzakeen. Horregatik, aurtengo urtarrilean, Wi-Fi Alliancek iragarri zuen WPA3 estandarra aterako zuela, eta ekainaren amaieran aurkeztu zuten.

WPA3a, arazoak konponduko dituena

Goian aipatutako WPA2aren arazo guztiak konpontzen ditu WPA3ak. Hasteko, pasahitz laburrak erabiltzen baditugu ere, WPA3an ezin da hiztegi-erasorik egin, hau da, ezin da pasahitz-mordoa probatu bata bestearen atzetik. Gainera, konektatutako gailu bakoitzak zifratze pertsonalizatua izango du, eta, pasahitza jakinik ere, hirugarren batek ezin izango du mezuak irakurri. Azkenik, gailu txikiak konektatzeko modu seguru bat definitzen du, routerrak eta gailuak izango dituzten QR kodeen bidez. Horrez gain, zifratzea 192 bitekoa izango da, lehengo 128 biteko zifratzearen ordez.

WPA3a definitu eta aurkezteak ez du esan nahi horrekin guztia konpontzen denik. Ekoizleek inplementatu egin beharko dute lehenik, eta Wi-Fi Alliance-k inplementazio horiek egiaztatu, ondoren. Eta, gero, horrek gure etxe eta enpresetako gailuetara iritsi beharko du. Ordenagailuetan ohikoak izaten dira eguneratzeak, telefonoetan ez hainbeste eta routerretan gutxiago; beraz, guztiek WPA3a izateko, gailu berriak erosi beharko dira, kasu askotan.

WPA3aren egileak oso ziur eta harro agertu dira bere segurtasunaz. Egia esan, aurrekoaren arazoak konpondu dituzte, eta ematen du ere etorkizunean pentsatu dutela. Baina historiak erakutsi digunez, ez dago sistema perfektu eta segururik, betirako iraungo duenik; kontua da zenbat denbora iraungo duen segurua izaten. Aurreko WPA2 protokoloak bezainbeste irauten badu, ez da gutxi izango. ●