Ffynhonnell: Cisco Meraki – Dadansoddiadau Lleoliad

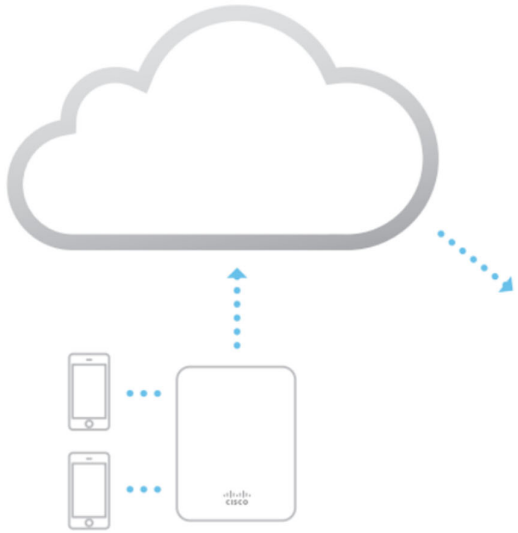
Gellir ffonau clyfar gyda WiFi bellach gael eu defnyddio fel dangosydd o bresenoldeb cwsmeriaid diolch i fecanwaith WiFi sy'n gyffredin ar draws pob dyfais o'r fath: **ceisiadau archwilio.** Mae'r fframiau rheoli 802.11 hyn yn cael eu trosglwyddo yn rheolaidd **o** ddyfeisiadau WiFi.

Mae'r fframiau'n cynnwys gwybodaeth y gellir ei ddefnyddio i nodi presenoldeb, amser a dreuliwyd, ac ailadrodd ymwelaidau o fewn cyrhaeddiad o unrhyw bwynt mynediad WiFi. Gellir canfod y dyfeisiadau hyn gan bwyntiau mynediad WiFi beth bynnag yw statws y WiFi sy'n golygu, **hyd yn oed os nad yw defnyddiwr yn cysylltu ei ddyfais/dyfais i'r rhwydwaith di-wifr**, gellir canfod presenoldeb y ddyfais o hyd tra bod y ddyfais o fewn cyrhaeddiad o'r rhwydwaith a bod antena WiFi y ddyfais ymlaen.

Device State	Probe Request Interval (smartphones)
Asleep (screen off)	~ once a minute
Standby (screen on)	10 - 15 times per minute
Associated	varies, could require user to manually search for networks

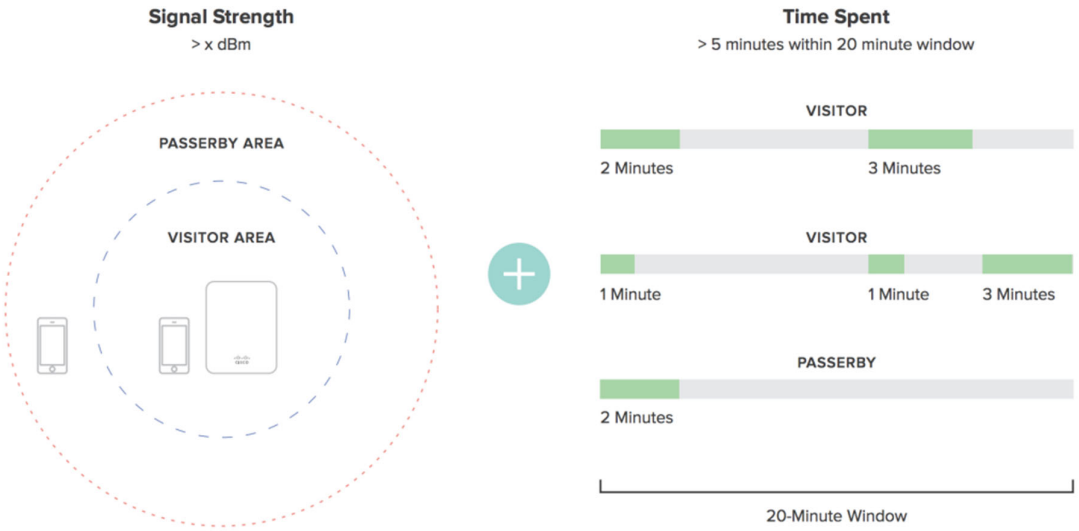
Table 1

Probe request interval seen on smartphone OS vendors (iOS, Android, others) - varies greatly based on apps, device upgrades, and other factors[4].



Probing and associated clients

Meraki's CMX Location Analytics



Mae Meraki yn defnyddio ceisiadau archwilio, fframiau data, a fframiau goleufa Bluetooth i leoli a storio lleoliad cleientiaid.

Gan fod y data lleoliad yn cynnwys cyfeiriadau MAC crai, gweithredodd Meraki nifer o **fecanweithiau diogelwch i ddienwi'r data mewn modd anwrthdroadwy.**

Gan ddefnyddio algorithm Meraki unigryw, mae'r cwmwl Meraki yn defnyddio proses '*hashes, salts and truncates*' ar gyfer cyfeiriadau MAC fel nad ydynt yn ganfyddadwy. Yna mae cwmwl Meraki yn storio'r fersiwn yma o'r cyfeiriadau MAC. Disgrifir y broses ddienw hon mewn mwy o fanylder isod.

Mae ffwythiant yr hash fel a ganlyn: Mae SHA1 yn ffwythiant cryptograffig unffordd sy'n cael ei adnabod yn eang. Defnyddio hashau SHA1 yn y modd hwn yw safon y diwydiant presennol. Er mwyn darparu haen ychwanegol o ddiogelwch y tu hwnt i hashio SHA1, mae ffwythiant hash Meraki yn cwtogi'r hash i 4 beit. Mae hyn yn cynhyrchu colled theoretig gwybodaeth, gan fod parth y ffwythiant yn fwy na'r amrediad: mae MAC 6-beit yn caniatáu (2 ^ 32). Mae hyn yn arwain at 65, 000 o gyfuniadau posibl (org + MAC) ar gyfer pob un cyfeiriad MAC 4-beit sydd wedi ei hashio. Felly, o ystyried MAC sydd wedi defnyddio proses '*hashes, salts and truncates*' gyda'r algorithm Meraki unigryw, byddai'n amhosibl yn fathemategol gwybod gyda gradd resymol o sicrwydd beth oedd cyfeiriad MAC y cleient gwreiddiol.

Mae'r ffwythiant hash yn arwain at golled theoretig gwybodaeth, **ac ni ellir byth adennill cyfeiriad MAC gwreiddiol cleient.**

Mae Cisco Meraki yn cynnwys org-gyfrinach penodol ar gyfer cwsmeriaid yn y ffwythiant hash. O ganlyniad, nid oes gan Cisco Meraki unrhyw weledded i ymddygiad cleientiaid ar draws ein rhwydweithiau cwsmeriaid ledled y byd. Ac, wrth gwrs, ni all unrhyw gwsmer Cisco Meraki weld dadansoddeg o sefydliad cwsmer arall neu ble mae traffig ar droed yn mynd ar ôl gadael presenoldeb ei rwydwaith WiFi / BLE ei hun.

Yn olaf, mae gwefan Cisco Meraki yn cynnig nodwedd optio allan byd-eang sy'n caniatáu i ddefnyddwyr gyflwyno cyfeiriadau MAC eu dyfeisiau, ac ar ôl hynny ni fydd y cwmwl Meraki yn canfod eu cyfeiriadau MAC naill ai ar gyfer ei Ddadansoddiadau Lleoliad sydd wedi ei fewn adeiladu

neu ar gyfer allforio amser real trwy'r API Sganio. Mae Cisco Meraki hefyd yn argymell bod manwerthwyr ac eraill sy'n defnyddio'r hysbysiadau post API Sganio ar argaeledd yr optio byd-eang hwn mewn lleoliadau amlwg, yn ddelfrydol ar flaen y siop neu wrth mynedfeydd adeiladau ble mae datgeliad lleoliad yn digwydd.