15 aastat hiljem: WiFi saab suurema turvalisuse ehk WPA3

6 years tagasi Autor: Kaido Einama

Aastal 2003 tuli Wi-Fi Alliance välja revolutsioonilise lahendusega - Wi-Fi Protected Access ehk laialt tuntud kui WPA tegi juhtmevabad võrgud turvalisemaks kui eales varem ja kohati räägiti lausa murdmatust turvalisusest, mida see tagas võrreldes vana standardiga. Tänapäeval ei soovita WEP-i enam keegi, kuid ka WPA2 on hea tahtmise juures häkitav. Sellepärast kinnitaski Wi-Fi Alliance nüüd, keset uimast südasuve uue standardi WPA3, mis fikseerib selle turvaaugu ja tagab parema salastatuse.

Miks WPA2 on ebaturvaline?

WPA2 on häkkides pealtkuulatav ruuteri läheduses. Õnneks kaug-rünnet pole WPA2-ga kaitstud WiFi-võrgule võimalik teha ja õnneks jäävad turvaliseks ka HTTPS-ühendused. Kuid pealt kuulata sinu WiFi-võrgu läheduses on võimalik, kui keegi peaks seda väga soovima. Vahendiks on **K**ey **R**einstallation **A**ttac**k**s ehk KRACK. Ja õnneks on sellele ka hulk *patch*e väljas. Kuid tegemist on üldise standardi probleemiga ja just sellepärast pidigi Wi-Fi Alliance välja töötama uue standardi WPA3.

WPA3 tuleb välja kahes versioonis: WPA-Personal ja WPA-Enterprise

KRACK-i kasutatav turvanõrkus on uues standardis loomulikult kõrvaldatud. Nüüd kasutatakse PSK ehk *Pre-shared Key* krüpteeringu asemel Dragonfly Key Exchange protokolli, mis esialgsete testide järgi on igatpidi turvaline.

Kui WPA2 puhul sai teha ülikiirelt tohutul hulgal päringuid salasõnadega massiliselt proovimiseks, siis nüüd tuleb iga vale salasõna järel ühendus uuesti luua, mis võtab aega ja vähendab proovimiste hulka. WiFi salasõnad on paljudel üsna nõrgad, seega on võimalik neid tihti ka tüüpiliste "sõnaraamaturünnakutega" ära arvata ehk enamlevinud salasõnu ja sõnaraamatusõnu proovides.

Samuti tugevdatakse ka ettevõtete WiFi krüpteeringut uute algoritmidega.

Mis nüüd saab?

Esialgu ei juhtu midagi, sest tootjad peavad alles hakkama uusi seadmeid WPA3-ga varustama. Ilmselt esimesed ruuterid saavad WPA3 kuskil selle aasta lõpus, laiemalt levib see järgmise aasta jooksul.

Uuele standardile üleminek on pea täielikult võimalik tarkvarauuendustega, kuid ilmselt käib uus tarkvara kõigepealt kaasa uuematele ruuteritele, hiljem tehakse *patch*id saadavaks ka vanematele seadmetele. Kui ruuter on WPA3 toega, oskab see ka WPA2 seadmetega edasi suhelda, nii nagu eksisteerisid WEP ja WPA kõrvuti.

Mida seni teha?

On selge, et seni peab hakkama saama WPA2-ga, mis võib hea tahtmise juures olla häkitav. Selle ajani, kui WPA3 välja tuleb, võiks...

- kasutada mobiilidel võimalusel WiFi asemel mobiilset andmesidet
- kasutada arvutis võimalusel VPN-i koduruuterisse
- külastada vaid HTTPS-iga kaitstud veebisaite, kui on oht privaatsete andmete lekkeks
- värskendada oma ruuteri ja WiFiga mobiilsete seadmete tarkvara

Vaata lähemalt WPA3 kohta siit.

- Uudised

- Andmeside
- Turvalisus

Pilt


Power
System
LAN
WLAN
QSS
QSS
N Access Point