WIFI MAC Filtering

Úvod

V súčasnej dobe je pripojenie pomocou bezdrôtovej siete viac a viac využívane a takmer v každej tretej domácnosti možno nájsť WIFI pripojenie. To však znamená, že bezpečnosť týchto sieti je veľmi žiadúca a bolo vytvorených niekoľko možných opatrení. Najpoužívanejšia je technika WPA (Wi-fi Protected Access), ide o štandard, ktorý poskytuje (s kombináciou vhodného šifrovania) dostatočne bezpečnú sieť. Ďalšou, často kritizovanou, alternatívou je použiť opatrenia založené na filtrovaní MAC adries. To môže uľahčiť administrátorovi siete prácu, avšak cena môže byť veľká.

Technika MAC Filtering

V prvom rade je dobre poznamenať, že MAC Filtering nie je štandard, tzn. nie je zahrnutý do štandardu 802.11. Ide iba o implementáciu, ktorú autori zahrňujú do prístupových bodov (AP) ako súčasť manažmentu. Princíp spočíva v tom, že každé sieťové zariadenie má pridelenú tzv. MAC adresu, ktorá je jednoznačná pre toto zariadenie. Filtrovanie je teda založené na povolení/zakázaní konkrétnych MAC adries a to pomocou tzv. blacklistu alebo whitelistu. Bežný scenár je, že administrátor pridá do whitelistu len tie MAC adresy, ktorým dôveruje. Prípadne do blacklistu pridá tie adresy, ktoré sú identifikované ako neznáme alebo bola zistená podozrivá aktivita.

Pokiaľ dôverujem klientom a tak trochu sa opieram o ích neznalosť o WIFI sieťach, tak môže byť táto metóda dostačujúca.

MAC Spoofing

Je jednou z techník ako získať prístup na bezdrôtovú sieť, ktorá využíva filtrovanie MAC adries. Technika spočíva v upravení samotnej MAC adresy na úrovni OS a za túto adresu sa vydávať. Útočník najprv odchytáva pakety, ktoré sú v tom čase prenášane v bezdrôtovej sieti (napr. pomocu airodump-ng) a cieľom je zistiť validnú MAC adresu. Po nájdení takejto adresy je už jednoduché maskovať MAC adresu a pripojiť sa na sieť. MAC spoofing je možno detekovať (napr. profilovaním OS, sieťového zariadenia, atď.) a spraviť dodatočné opatrenia. Nie je to však jednoduchá záležitosť.

Úroveň zabezpečenia

Filtrovanie podľa MAC adries samo o sebe nezaručuje šifrovanú komunikáciu. Je to len nástroj pre obmedzenie prístupu k sieti na základe MAC adresy. Je to obecne slabá technika a nikdy by nemala byť považovaná za bezpečnú, pokiaľ nie je používaná spolu so štandardom spomenutým v úvode.

Kedy používať filtrovanie MAC adries?

- V prípade statickej sieti, tzn. klienti sú známy a nie je vysoký nárast nových klientov. Napríklad v bežnej domácnosti.
- Z nejakého dôvodu nechcem používať šifrovanie, avšak sieť chcem udržovať bezpečnú ako to je možné. S týmto som sa stretol len v prípade, že signál AP bol príliš slabý a na strane klienta bolo treba dešifrovať, už aj tak na slabom HW, čím bola mierne zvýšená latencia – zrejme úplne krajný prípad.
- Obecne prípady, kedy je dobré použíť MAC Filtorvanie sú zriedkavé. Väčšinou ide len o akési vylepšenie už dostatočne zabezpečenie WIFI siete. Môže to byť teda individuálne.

Záver

Na záver by som ešte raz zdôraznil, že použitím MAC Filteringu nezískam bezpečnú sieť, iba tým odradím neznalých klientov. Ak je to možné (čo v súčasnosti je vždy), tak je lepšie používať dostatočne silné šifrovanie, či už s kombináciou filtrovania alebo nie, a nespoliehať sa na neznalosť ľudí.

Literatúra

http://en.wikipedia.org/wiki/MAC_filtering

http://en.wikipedia.org/wiki/MAC_spoofing

Zaujímaví text o MAC filteringu

http://www.wi-fiplanet.com/tutorials/article.php/3924486/MAC-Filtering-for-Your-Wireless-Network.htm

Jerguš Lysý, 374217