

MAC filtering

In computer networking, **MAC Filtering** (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network.

MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists. While the restriction of network access through the use of lists is straightforward, an individual person is not identified by a MAC address, rather a device only, so an authorized person will need to have a whitelist entry for each device that he or she would use to access the network. [1]

MAC address forgery(MAC spoofing)

It is possible to scan for a valid MAC address on a wireless network and then use it to connect to the network. We can use airodump-ng to determine connected client to the network and change our MAC address to be accepted by MAC filter. How to use airodump-ng you can find in aircrack-ng documentation[2]. In linux MAC address can be changed by following commands:

```
# ifconfig eth0 down
# ifconfig eth0 hw ether <your new MAC address>
# ifconfig eth0 up
# ifconfig eth0 |grep HWaddr.
```

In windows MAC address can be changed in wireless adapter settings or in registry under register key: "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}". If you change your MAC address in registry it is necessary to reboot your computer.

Preventing MAC spoofing

It is possible to identify spoofed MAC address based on higher layer information or on received signal properties. Collecting profiling information as client operating system type, platform, location, time, signal strength, response time and many others we can identify spoofed MAC address.

Conclusion

MAC Address filtering is often referred to as Security through obscurity and mainly on wireless networks it can lead to a false sense of security. To protect access to wireless network use rather WPA or WPA2[3].

References

- [1] Wikipedia. MAC filtering. 2014. url: http://en.wikipedia.org/wiki/MAC_filtering
- [2] Aircrack-ng. Airodump-ng. 2014. url: <http://www.aircrack-ng.org/doku.php?id=airodump-ng>
- [3] Wikipedia. Wi-Fi Protected access. 2014. url: http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access