WIKIPEDIA

MAC spoofing

MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device. The MAC address that is hard-coded on a network interface controller (NIC) cannot be changed. However, many drivers allow the MAC address to be changed. Additionally, there are tools which can make an operating system believe that the NIC has the MAC address of a user's choosing. The process of masking a MAC address is known as MAC spoofing. Essentially, MAC spoofing entails changing a computer's identity, for any reason, and it is relatively easy.[1]

Contents

Motivation

The changing of the assigned MAC address may allow the bypassing of access control lists on servers or routers, either hiding a computer on a network or allowing it to impersonate another network device. MAC spoofing is done for legitimate and illicit purposes alike.

New hardware for existing Internet Service Providers (ISP)

Many ISPs register the client's MAC address for service and billing services.[2] Since MAC addresses are unique and hard-coded on network interface controller (NIC) cards,[1] when the client wants to connect a new gadget or change his/her existing gadget, the ISP will detect different MAC addresses and the ISP might not grant Internet access to those new devices. This can be circumvented easily by MAC spoofing. The client only needs to spoof the new device's MAC address to the MAC address that was registered by the ISP.[2] In this case, the client spoofs his or her MAC address to gain Internet access from multiple devices. While this seems like a legitimate case, MAC spoofing new gadgets can be considered illegal if the ISP's user-agreement prevents the user from connecting more than one device to their service. Moreover, the client is not the only person who can spoof his or her MAC address to gain access to the ISP. Hackers can gain unauthorized access to the ISP via the same technique. This allows hackers to gain access to unauthorized services, and the hacker will be hard to identify because the hacker uses the client's identity. This action is considered an illegitimate use of MAC spoofing and illegal as well.

However, it is very hard to track hackers that are utilizing MAC spoofing.[3]

This also applies to customer-premises equipment, such as cable and DSL modems. In cases where the provider leases the equipment to the customer on a monthly basis, the CPE has a hard-coded MAC address which is on a list known to the provider's distribution networks, allowing service to be established as long as the customer is not in billing arrears. In cases where the provider allows customers to provide their own equipment (and thus avoid the monthly leasing fee on their bill,) the provider requires that the customer give them the MAC address of their equipment before service will be established.

Fulfilling software requirements

Some software can only be installed and run on systems with pre-defined MAC addresses as stated in the software end-user license agreement, and users have to comply with this requirement in order to gain access to the software. If the user has to install different hardware due to malfunction of the original device or if there is a problem with the user's NIC card, then the software will not recognize the new hardware. However, this problem can be solved using MAC spoofing. The user just has to spoof the new MAC address as to mimic the MAC address that was registered by the software.[4] This activity is very hard to define as either legitimate or illegitimate reason for MAC spoofing. Legal issues might arise if the user grants access to the software on multiple devices simultaneously. At the same time, the user can obtain access to software for which he or she has not secured a license. Contacting the software vendor might be the safest route to take if there is a hardware problem preventing access to the software. Software may also perform MAC filtering because the software does not want unauthorized users to gain access to certain networks to which the software grants access. In such cases MAC spoofing can be considered a serious illegal activity and can be legally punished.[5]

Identity masking

If a user chooses to spoof his or her MAC address in order to protect the user's privacy,[4] this is called identity masking. One might wish to do this because, as an example, on a Wi-Fi network connection a MAC address is not encrypted. Even the secure IEEE 802.11i-2004 (WPA) encryption method does not prevent Wi-Fi networks from sending out MAC addresses.[4] Hence, in order to avoid being tracked, the user might choose to spoof the device's MAC address. However, hackers use the same technique to maneuver around network permissions without revealing their identity. Some networks use MAC filtering in order to prevent unwanted access. Hackers can use MAC spoofing to get access to a particular network and do some damage. Hackers' MAC spoofing pushes the responsibility for any illegal activity onto authentic users. As a result, the real offender may go undetected by law enforcement.[4]

MAC Address Randomization in WiFi

To prevent third parties from using the MAC address to track devices, Android, Linux, iOS, and Windows[6] have implemented MAC address randomization. In June 2014, Apple announced that future versions of their iOS platform would randomize MAC addresses for all WiFi connections. The Linux kernel has supported MAC address randomization during network scans since March 2015,[7] but drivers need to be updated to use this feature.[8] Windows has supported it since the release of Windows 10[6] in July 2015.

Controversy

Although MAC address spoofing is not illegal, its practice has caused controversy in some cases. In the 2012 indictment against Aaron Swartz Internet hacktivist, who was accused of illegally accessing files from JSTOR digital library, prosecutors claimed that because he had spoofed his MAC address it showed purposeful intent to commit criminal acts.[5] In June 2014, Apple announced that future versions of their iOS platform would randomize MAC addresses for all WiFi connections, making it more difficult for internet service providers to track user activities and identities, which resurrected moral and legal arguments surrounding the practice of MAC spoofing among several blogs and newspapers.[9]

Limitations

MAC address spoofing is limited to the local broadcast domain. Unlike IP address spoofing, where senders spoof their IP address in order to cause the receiver to send the response elsewhere, in MAC address spoofing the response is usually received by the spoofing party if switch is not configured to prevent MAC spoofing.

See also

- MAC address
- Promiscuous mode
- IP spoofing
- ifconfig, linux utility capable of changing MAC address

References

1. Cardenas, Edgar D. "MAC Spoofing--An Introduction" (http://www.giac.org/paper/gsec/3199/mac-spoofing-an-introduction/105315). *GIAC Security Essentials Certification*. SANS Institute. Retrieved 8 February 2013.
2. "MAC Spoofing" (https://web.archive.org/web/20120623060142/http://www.rcmp-grc.gc.ca/ncecc-cncee/factsheets-fichesdocu/macspoof-usurpmac-eng.htm). *Royal Canadian Mounted Police*. Research and Development Section in Collaboration with the NCECC's Technology Unit. Archived from the original (http://www.rcmp-grc.gc.ca/ncecc-cncee/factsheets-fichesdocu/macspoof-usurpmac-eng.htm) on 23 June 2012. Retrieved 8 February 2013.
3. Gupta, Deepak; Gaurav Tiwari (4 November 2009). "MAC SPOOFING AND ITS COUNTERMEASURES" (http://ijrte.academypublisher.com/vol02/no04/ijrte02041721.pdf) (PDF). *International Journal of Recent Trends in Engineering*. **2** (4): 21. Retrieved 8 February 2013.
4. Pahwa, Payal; Gaurav Tiwari; Rashmi Chhabra (January 2010). "Spoofing Media Access Control (MAC) and its Counter Measures". *International Journal of Advanced Engineering & Application*. India: 186–192.
5. Indictment against Aaron Swartz (https://www.wired.com/images_blogs/threatlevel/2012/09/swartzsuperseding.pdf)
6. http://papers.mathyvanhoef.com/asiaccs2016.pdf
7. https://w1.fi/cgit/hostap/plain/wpa_supplicant/ChangeLog
8. https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=ad2b26abc157460ca6fac1a53a2bfeade283adfa
9. Change MAC Address: Use Public WiFi Signals Without Any Limits, Not To Mention Serious Privacy Benefits (http://www.collegetimes.tv/change-mac-address/)