# Chapter V
# Wireless Wardriving

**Luca Caviglione**
*Institute of Intelligent Systems for Automation (ISSIA)—Genoa Branch, Italian National Research Council, Italy*

## ABSTRACT

*Wardriving is the practice of searching wireless networks while moving. Originally, it was explicitly referred to as people searching for wireless signals by driving in vans, but nowadays it generally identifies people searching for wireless accesses while moving. Despite the legal aspects, this "quest for connectivity" spawned a quite productive underground community, which developed powerful tools, relying on cheap and standard hardware. The knowledge of these tools and techniques has many useful aspects. Firstly, when designing the security framework of a wireless LAN (WLAN), the knowledge of the vulnerabilities exploited at the basis of wardriving is a mandatory step, both to avoid penetration issues and to detect whether attacks are ongoing. Secondly, hardware and software developers can design better devices by avoiding common mistakes and using an effective suite for conducting security tests. Lastly, people who are interested in gaining a deeper understanding of wireless standards can conduct experiments by simply downloading software running on cost effective hardware. With such preamble, in this chapter we will analyze the theory, the techniques, and the tools commonly used for wardriving IEEE 802.11-based wireless networks.*

## THE (ART OF) WARDRIVING

Owing to the absence of physicals barriers, the wireless medium, and consequently wireless (WLANs) are accessible in a seamless manner. Thus, checking for the presence of some kind of wireless connectivity is quite a natural instinct; it is sufficient to enable the wireless interface and wait. This action is a very basic form of wardriving, a term originally coined by Shipley (2000) to refer to the activity of "driving around, looking for wireless networks." This activity rapidly evolved, and nowadays it implies three basic steps: (1) finding a WLAN, (2) defining precisely its geographical coordinates by using GPS devices, and (3) publishing the location in specialized Web sites to enrich the wardriving community.

With the increasing diffusion of WLANs, especially those based on the cost effective IEEE 802.11 technologies, searching for wireless signals is a quite amusing and cheap activity. However, the IEEE 802.11 family originally relied (and still relies) on weak security mechanisms. In addition, many users unconsciously operate their wireless

networks without activating any confidentiality, integrity, and availability (CIA) mechanisms: opportunity makes the thief. Then, wardriving becomes a less noble hobby, since many wardrivers try also to gain access to the discovered networks; many of them are only interested in cracking the network, while a portion will steal someone else's bandwidth. In this perspective, another basic step has been introduced: (4) trying to gain access to the WLAN.

It is also interesting that wardriving is becoming part of the urban culture. For instance, it spawned a strange fashion called *warchalking*, that is, *the drawing of symbols in public places to advertise wireless networks*, as defined by Matt Jones (as cited in Pollard, 2000).

*Then, why is it important to know about wardriving?*

Firstly, because you must become conscious that an active WLAN can trigger "recreational activities," even if it is solely employed to share a printer. Secondly, the coordinated effort of many people highlighted several security flaws in the IEEE 802.11 standards and produced effective tools to test (well, actually, to compromise) the security of access points (APs). Thirdly, while performing their "raids," *wardrivers* discovered flaws in the devices; consequently, this is a valuable knowledge that could be used to avoid further errors. Lastly, trying to be a wardriver is an instructive activity that will help to better understand WLANs technologies, develop your own auditing tools and procedures, and prevent, or at least, recognize attacks.

## HARDWARE AND SOFTWARE REQUIREMENTS

In the basic form of searching for a WLAN, the act of wardriving could be simply performed by having a device equipped with an IEEE 802.11 air interface. Then, one can use a standard laptop, a wireless-capable console, or a handheld device. However, the typical gear consists of a laptop and a GPS device (even if not strictly necessary). Nevertheless, many wardrivers do prefer a Personal Computer Memory Card International Association (PCMCIA) wireless card that is capable to connect with an external antenna to sense a wider area. With this basic setup you should be able to enable the wireless interface and start scanning the air. But, in order to conduct more sophisticated actions, a deeper understanding of aspects related to hardware and software should be gained. A detailed breakdown follows.

### Wireless Interfaces

Each model of wireless interface differs in some way. Regardless of different power consumption, better antennas, and so on, two major aspects must be taken into account: the chipset and the availability of ad hoc drivers. The chipset roughly represents the soul of a wireless interface and it is mostly responsible of its capability. For instance, some chipsets do not allow assembling ad hoc frames, preventing from exploiting particular attacks. The reasons are different: the chipset could lack the logic to deal with raw packets or its specification is not known, discouraging tool developers to exploit such functionalities. At the time of this writing, cards based on the Prism chipset are the most studied and documented, resulting in a variety of pre-made tools for preparing packets.[1] Lastly, being the interfaces engineered for providing connectivity and not such kind of tasks, manufacturers often change the internal chipset, even if maintaining the model or the brand name. This is why not all wireless cards are the same, and you should check their specifications carefully if you plan to use them for wardriving.

### Device Drivers and Scanning

Device drivers provide the basic bridge between the user software and the hardware. Having a flexible device driver is mandatory to reach the soul of your interface. The best device drivers for wardriving are available for the aforementioned chipset, and for Unix systems. In addition, owing to its open source nature, Linux has the best available drivers.