Wardriving legal issues

The paper “ Security of the Wireless Networks at Home and in the Office" is a persuading example of a term paper on information technology. With the passage of time, there is explosive development in wireless computing, both in the organizations and at home, and this presents totally different security problems. The security problem of Wireless networks is different in homes as compared to organizations. In the organizations' individuals setting up the network sometimes fail to understand the security requirements. The equipment of wireless networks comes with a default setting configured by the manufacturer. If this default setting is not changed then it gives benefit to hackers. Hackers, who know the default setting, can gain access to a wireless network. In this way, the network fails to require identification and verification of all users. Many Government and private sector organizations have installed high-speed wireless networks. However, there is substantial variation in the security measures built into these networks.

According to Chris Hurley WarDriving is “ the act of moving around a precise area and mapping the population of wireless access points for statistical ideas.” In the definition, Wardriving does not mean to drive around in a car. It means to drive around in a specific area for getting an idea about data. Citizens have war driven just by walking around in a region with a PDA, or with the help of a laptop while taking a taxi or the subway.

Chris Hurley is one of the originators of the yearly DefCon Wardriving Contest. The contest now held in Las Vegas, where thousands of people from all over the world meet each year to converse issues concerning among other things wireless security. The first DefCon war drives took place in 2002, and 21 teams participated in having more than eighty contestants. The rules were relatively straightforward; the criteria for awarding points was

based on the following based on factors, listed below:

- There was one given for every Access Point.

- Two extra points for A. P.’s with default SSID and no WEP enabled.

- Five extra Points for A. P.’s that were found by only one group.

All the groups were restricted to four group members and allowed only two hours in which to drive. The contest was very successful and is now carried out every year. Black DefCon badge is the name of the award that is given to the winning team. Only challenge winners obtained badges and they have become a cherished part of DefCon memorabilia.

For war driving today very little is required in terms of equipment. For this purpose they must have a laptop with a wireless card or a new computer for this function can be purchased very inexpensively now, software designed to monitor the networks, and a GPS unit. Software is available for a range of devices and operating systems; from Windows to a palm pilot.

In the past, when dial-in use was common and corporate networks had their own pools of modems, attackers would use a technique called " war-dialing" in which scripts would create huge chunks of random phone numbers and dial them, trying to locate a phone that would respond with a modem connection string. This type of mass dialing moved itself onto the Internet on one occasion the latter became the prevalent way of accessing information and computers, and it became even more ordinary and also more helpful by permitting attackers to not even need a phone line to knock on the doors of groups of computers, establish by randomly generating their Internet Protocol address.

Presently, a number of illegal methods of accessing wireless networks, another legal method are quickly increasing in popularity. Several

organizations now present wireless access to their customers. The collection of businesses is large, varying from car dealerships to a large range of restaurants, coffee shops, and hotels. Thousands of Starbucks across the country have Wi-Fi points accessible through T-Mobile. It should be noted that wireless hotspots accessible to T-Mobile are supported by the 802. 1x standard and give support to WPA. It is the consumer’s responsibility to put into practice these protections.

In the present, wireless networks have suddenly become the target of Wardrivers. With the help of special software, an attacker can drive through any city or populated area, sampling the airwaves for wireless access points. Special wardriving software maintains information concerning latitude, longitude, and configuration of the access points establish along the driver's route. This is an important thing to keep in mind when deploying your WAPs. Further laws are being devised, which would move at least some of the legal encumber of wireless networks to their owners. A law is waiting in Westchester County New York which would involve businesses which offer wireless internet connections to make use of encryption. The law, which gives a warning for the first infringement and then rising fines, is projected to protect consumers from identity theft.

Wireless networking is the latest technology that is growing tremendously over the last few years. As with approximately all parts of technology, there are those who have used it for unlawful purposes; yet it seems unambiguous that a greater part of those using wireless networks is doing so with authorization. There are great expectations that in the coming decade as the number of access points maintain to go up that so will the numbers of protected access points also will go up.