Status Of Wireless Network Security
In The
Fredericksburg Virginia Area

Brought to you by
Defcon-5
www.defcon-5.com

Last updated:
June 08, 2004

Table of Contents

Introduction

Defcon-5 is local security consulting firm based out of Spotsylvania Virginia. Defcon-5 was hired to perform an analysis for a customer of the security of their wireless network. During this analysis Defcon-5 was to identify any wireless access points the customer had, and secure them. While in this process other wireless networks where able to be detected unintentionally.

Defcon-5 had found that the customer also had other wireless networks in very close proximity to them. The tools and software that Defcon-5 used to help survey the customer's wireless network to see if it was secure, also picked up the security status of other wireless networks.

This scan does not attempt to access any part of the wireless network, it just simply makes a request to say the equivalent of "Hello I am here is anyone else here?" When a wireless access point responds it will provide it's SSID (if configured to do so), and if it is running any kind of wireless encryption such as WEP, or WPA.

What surprised Defcon-5 was that out of the five other wireless networks they found while performing this analysis for their customer, all but one was left unsecured with no encryption. What this means is that basically anyone could walk up to one of these wireless networks and simply access the network with as little effort as turning on their computer.

Amazed at how many unsecured wireless networks could be in one small area Defcon-5 decided to perform a survey of wireless network in the Fredericksburg Virginia area to see what percentage of wireless networks were unsecured in the area.

Area Covered

Defcon-5 has tried to balance out the types of areas that the survey covers as far as percentage of residential, and business centric locations such as Central Park. Suburbs, and apartment complexes have been included in parts of the survey as well to balance out the spectrum of individuals that could potentially be using a wireless network. In order to do this some parts of Stafford, Spotsylvania, and Fredericksburg were surveyed. Defcon-5 being a security consulting firm understands that protecting information can be a valuable step in security, hence names of specific suburbs and residential areas will not be mentioned in case potential attackers (hackers, spammers, etc.) are reading this document. In addition no specific addresses will be mentioned as well. Defcon-5 values the privacy of its customers, other businesses, and citizens as well, because of this no other company names or customer information will be provided in this document as well. We have excluded the map from this document to help prevent malicious activity.

Survey Process

Using the same software as Defcon-5 usually uses for detecting rouge wireless networks for customers, and a standard 802.11x card (This one in particular supports 802.11a, b, and g), which is also used in a normal detection process as well, Defcon-5 simply placed this setup in a car and drove through the survey areas. In order to map the wireless access points a GPS (Global Positioning System) and mapping software was integrated into the setup. Looking at the map generated it is possible to see where the majority of wireless networks are located (residential or business areas). These maps were generated from the logs created by the wireless detection software, which polled the GPS for positioning data every two seconds. While not 100% accurate as far as mapping placement of the wireless networks, it is still considerably accurate, and good enough for the intention of the mapping.

Over the course of several days information was gathered by driving through various residential and business areas. All of the driving was done on weekends, and during the day when the majority of individuals would be using their networks to make sure the maximum number of networks could be detected. Surveying began at around 10:00 AM, and stopped at around 2:00 PM each day (four hours each session). The survey was conducted three Saturdays in a row.

The survey process, and time ranges are simple and easy to replicate, and the hardware used can be any basic laptop with any decent 802.11 wireless network card will work. While the survey only managed to cover a handful of locations a larger survey could be expected to return similar results.

Survey Results

The results of this small survey are quite astonishing. Over the course of the three sessions, 388 wireless access points were found. The majority of these turned out to be in residential areas such as apartment complexes, and in the suburbs.

Based upon the location of these access points on the map, an approximate count of 240 (about 60% of all the wireless access points that were found) of these access points are residential. Leaving 148 (about 40%) of the access points found being used by businesses. The SSID's (Secure Set Identifier) of the wireless access points helps confirm this as well. Those that are in more residential areas have SSIDs that are first names, names of television shows, and names of various video games. While those that are in business areas have names that better match the company such as the company name.

Unfortunately due to the mapping software used, a break down cannot be done of what percentage of the residential and business groups use security in their wireless networks (For example it cannot be said that x% of all residential networks are not secured). However looking at the map it can be seen based on the color coding that the majority of the wireless networks found in residential areas were not secured. A manual count can be performed, however that is very prone to error. Business areas on the map visibly show more secured networks than residential areas, however this can be due to the lack of quantity when compared to residential wireless access points.

It is possible to get an overall comparison of secured wireless networks versus non-secured wireless networks. Using various filters available in the wireless scanning software, it is possible to get numbers for the total quantity of secured and non-secured wireless networks. A total of 247 access points were unsecured, and 141 were identified as being secured, indicating that almost 63% of all wireless networks surveyed are unsecured.

Another interesting note is the number of wireless access points that used the default SSID that ships with it. 153 of the 388 wireless access points found used the default SSID that is preconfigured from the factory. This is more interesting than the number of unsecured networks because this is a good indicator that a large percentage of wireless network owners are simply purchasing the wireless access point, turning it on, and leaving it. Meaning that the devices are most likely not secured at all. Manually counting the number of access points in this category that were secured is reasonable. A total of 10 access points with default SSIDs were actually secured. This could indicate that the owner of the access point did not want to change the SSID, or had no reason to. However the other 143 access points were not secured at all, more of an indication of a simple “take it out of the box and turn it on” issue. This would allow an attacker to change settings on the access point by using default login information, and other general well-known information about the device. Potentially causing a denial of service to the owner of the device as they may be kicked out of their own network.

Result Analysis

Reviewing the results of this survey by itself can provide a general idea of the status of wireless networks in the Fredericksburg Virginia area, however an analysis will provide a more in-depth look at what all the information really means.

The fact that 143 of the access points that were discovered had default SSIDs and were not secured is a strong indication of individuals purchasing wireless access points and simply taking them out of the box and turning them on. If you combine this with the fact that almost 63% of all the wireless networks that were surveyed were not secure, and the fact that about 240 of the access points found were in residential areas; it seems to be that the increase in the use of wireless networks has grown because they have become so simple to implement for individuals. This has turned the average installation procedure for a wireless access point into take it out of the box, plug it in and use it. While it is understandable that an access point should be quick and easy to get running, it should also be understood that not securing a wireless access point could be very dangerous.

Because the majority of the wireless networks that were found were in residential areas it is understandable that these are owned and managed by the average Joe homeowner. Hence it cannot be expected that the person who purchased and installed the access point be up on the latest information on configuring, and securing such devices. It is because of this more attention, and information on this subject should be made available to the public to let them know how easily their wireless network could be compromised.

Given also that it is common knowledge that most owners of wireless access points have a high-speed Internet connection such as cable, or DSL it is important to inform the public of what can be done with a compromised wireless network. Using a non-secured wireless network is a good choice for hackers, spammers, and virus writers to use to launch their attacks. For them it is very low risk, all they need is a laptop, wireless card, and some spare time to find wireless networks from which they can launch their attacks. The issue here is this gives the attacker another layer of which they can hide behind to remain anonymous, making it harder to track down the real culprit as it will appear to be the average Joe homeowner launching the attack because it came from his network. In addition with the high density of wireless networks in residential areas a resourceful attacker could utilize multiple systems to access several wireless networks at once, allowing for a larger attack base. In the end this hurts everyone, viruses can be launched easier and faster, hackers have an extra layer they can hide behind, and spammers have more network connections and bandwidth to use to send spam.

The best corrective measure would be for the manufacturers of wireless access points to include a notice in the package for the device informing their customers that they need to secure the device to protect themselves. Another step would be to ship the devices in a more secure state, however it is possible that could be more confusing to the end user as far as configuration goes. Either way the wireless device makers are in the best position to educate the public about such issues. Security consulting firms such as Defcon-5 are unfortunately only called in to correct such issues after an intrusion has been detected; pro-active security is the best solution for keeping intruders out. Learning that you could have protected yourself from such attacks with a few spare minutes of your time is too late if you have already been attacked.

Conclusion

Considering the quantity, and location of the majority of un-secured wireless networks, it is quite possible that they have been compromised and the owners of the wireless access points do not even know that they have been attacked. It cannot be expected for the average person to have all the necessary skill to configure the average access point. Because of this improving security out of the box for wireless access points is an essential step to securing the wireless networks of the future for individuals and businesses. Defcon-5 should conduct a larger survey to include more wireless networks at a later date. A larger survey will provide a better picture of the entire status of wireless networks as far as security configurations. However it can be expected that it will return similar results to this small survey.

In summary Defcon-5 has made the following conclusions:

1. Access point vendors are in the best position to inform the public about the security risks of using such devices. Hence they should include a notice with their products mentioning how important it is to secure the device, and to include the steps that someone needs to go through to do so.
2. Access points and wireless cards do not seem to have a similar simple interface that is easy to find, for the average individual to use in securing their devices. These interfaces need to be made similar in look and feel, and at the same time be simple and easy to find. This has been improving over the last couple of years fortunately.
3. Just like with most other attacks, individuals with high-speed Internet connections are a prime target for attackers because they often are not aware of how to secure their systems. Improved education of the public is necessary for not only the security of wireless networks but also the security of computer systems in general. Until then it appears to be that the average access point contained in a home is the most likely to be unsecured.
4. Some people will not implement wireless security such as WEP because they believe it to be un-secure. Given that WEP has been broken and can be done with some effort, it is still better to have than nothing at all as it increases the skill level and time needed to break into the network. However better standards such as WPA are much more difficult to break and provide much better security overall.
5. While the businesses in the Fredericksburg Virginia area have better wireless security than the individuals, there is still quite a few that are not secured. This just goes to show that everyone can use increased knowledge, and training on securing their wireless networks.

In the end this survey does match other research that claims anywhere between 40%-70% of wireless networks are not secured in any manner. A basic search on the Internet can yield a multitude of reports that have similar numbers to this survey.