ISSN: 2321-7782 (Online)
Volume 2, Issue 1, January 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Paper / Case Study
Available online at: www.ijarcsms.com

RAP Problems and Solutions in 802.11 Wireless LAN

Ajay M. Patel[1]
Assistant Professsor
Acharya Motibhai Patel Institute of Computer Studies
Ganpat University
Kherva - India

Ashok R. Patel[2]
Director
Department of Computer Science
Hemchandracharya North Gujarat University
Patan - India

Hiral R. Patel[3]
Assistant Professor
Department of Computer Science
Ganpat University
Kherva - India

Abstract: ***Wireless local area networks are becoming increasingly popular. The popularity of 802.11 Wireless LAN causes some serious threats due to some weakness in configuration and implementation of wireless network. There are several potential problems with allowing end users to add wireless or other devices to the company network without approval. One big one is they may not employ the proper security measures. There are also the issues of maintaining control of the organizations' infrastructure. Such devices which have been configured without approval of network administrator termed as a rouge access point. Those may cause serious security related issues for organization network. This Paper represents the wireless network attacks mainly based on rogue access points and provide some solution to overcome rogue access point problems.***

Keywords: ***Radio Frequency Jamming, Rogue Access Points, SSID, Wireless Attacks, Wireless Network.***

I. INTRODUCTION

When the term wireless security comes, 802.11 networks, 802.11, or the Institute of Electrical and Electronic Engineers (IEEE) 802.11, the standards defined for radio communications used in wireless local area networks or WLANs is also pronounce. IEEE uses the number 802 to define standards for local and wide area networks, while the number 11 narrows that down to wireless area networks. 802.11 networks are everywhere. The number of shipped 802.11-enabled hardware devices is estimated to exceed 200 million units by the year 2012 (Vladimirov, Gavrilenko, Mikhailovsky). Due of the wide end user acceptance of this communications standard and its prevalence in the world of organizational wireless networking, our focus in this text will be primarily on 802.11 WLANs. The wide acceptance of 802.11 WLANs also attracts intruders and it's natural. With the increasing deployment of the 802.11-based wireless Hotspots, their security continues to be a big concern.

II. RELATED RESEARCH REVIEW ON WLAN ATTACKS

The lot of research is ongoing for security perspective in the field of networking. In this topic of research paper the current status of ongoing trends is discussed.

A. CLASSIFICATION OF WIRELESS NETWORK ATTACKS

Wireless attacks exploit and influence computing and/or wireless network resources. They are able enough to degrade the wireless network performance and destroy the users' privacy. This section represents the survey of wireless attacks and counteractive approaches.

Wireless network attacks can be classified into four categories mainly: (RAP) Rogue Access Point, War Driving, Incorporating SSID, and Radio Frequency Jamming. A Rogue Access Point is one connected to a network without authorization from an administrator. RAPs have become a challenging issue in wireless security. With low-end access points steadily decreasing in price and increasing in availability, RAPs have become much more common. Additionally, many of these access points contain features that make them nearly invisible when coupled with legitimate networks, doing a fine job to conceal their presence.

Since RF (radio frequency) is essentially an open medium, jamming can be a huge problem for wireless networks. Jamming is one of many exploits used compromise the wireless environment. It works by denying service to authorized users as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic. A knowledgeable attacker with the right tools can easily jam the 2.4 GHz frequency in a way that drops the signal to a level where the wireless networks can no longer function.

SSID (Service Set ID) is a configurable identification mechanism that enables a client to communicate with the correct base station; all stations come included with their own default SSID. When configured properly, only clients configured with the corresponding SSID can interact with the base station. An attacker can exploit the default SSIDs in attempt to access a base station that may have still have its default configuration. Some will change the default SSID password to something simple, ultimately making the network just as vulnerable.

War driving is the perfect alternative when a wireless network attack seems next to impossible. The practice of war driving first achieved popularity in 2001, around the same time wireless network scanning tools became widely available. The initial war driving tools included simple software coupled with the WNIC (Wide-area Network Interface Coprocessor). In actuality, these programs were not designed with potential attackers or security professionals in mind. The inefficiency of these products sparked a need for more reliable solutions. However, war drivers have not completely dropped the use of WNIC-based software as it is still relevant in modern programs.

B. PRESENT WIRELESS SECURITY AT GLANCE

With the network's basic defences deployed and maintained, technical teams can shift their attention to the subject of defending the network from attacks. Attacks can come in a variety of forms, and in many cases can even be unintentional. Wireless LANs by their very nature provide a way of accessing the network through walls and physical barriers that normally protect business assets. Add this to the fact that most WLANs are not properly secured, and it is no wonder that an intruder would look to the wireless network as the ideal place to begin an attack .For several years now the industry has been developing hardware and software to support the 802.11 environment. The Wired Equivalent Privacy (WEP) protocol, 64 bit encryption, was introduced with a number of flaws in its security mechanisms and industry took a hard look at implementation of wireless environment based on the fears associated with the security flaws. The WEP protocol is being replaced by the new WPA (Wi-Fi Protected Access), and WPA/2 128 bit encryption security standard introduced. Additionally, a number of companies began to produce products to assist in overcoming the flaws inherent in WEP and to define standards for implementation and use of wireless tools to support the secure day-to-day business of large and small organizations.

The Wi-Fi alliance provides a list of products that have been released with the WPA standard, several that provide alternative security solutions like VPN and other mobile security measures and there are several other tools which meet the criteria established by the FIPS 140-1 and 140-2 guidelines for encryption. This Paper is focused on to study RAP (Rogue Access Point) problems with present security and the defensive step to overcome from it.

III. ROGUE ACCESS POINTS

As discussed earlier, it is easy for even a novice to acquire equipment and set up a wireless network. If this is done from within another network, it creates what is known as a subnet, which can create back doors to its parent. There are many easily

overlooked mistakes that can be made in configuring a wireless network, many of which novice users will overlook. Individuals who wish to intrude upon a network can also plant rogue access points themselves.

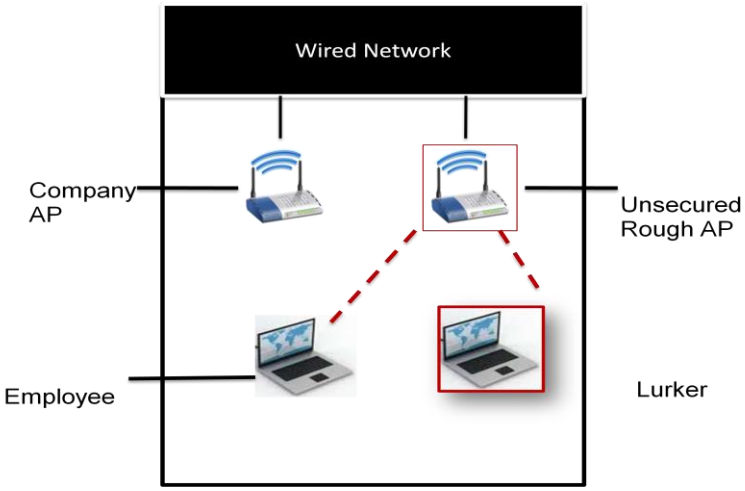

Fig. 1 Unsecured rouge access point allows anyone to connect to the network

The problem of rogue access points has garnered more attention in the industry than any other security issue, and for good reason. A rogue access point is any access point in your network that was not intentionally deployed by network staff. They can come from well-meaning employees who bring in devices from home, they can be devices used by attackers for malicious purposes, or they can be neighboring devices that simply overlap with your wireless network. These devices can have many effects and none of them are good in terms of network security. The most common rogue AP scenario involves devices introduced by employees. In this case, the employee brings in an unsecured access point, plugs it in to an available wired port and now has wireless access to the larger wired network. Unfortunately, so does anyone else within range of the access point including the wireless lurker in the parking lot. This provides virtually unchecked access to the entire enterprise network (Fig. 1). An attacker could pursue the strategy described above by planting a rogue device inside the building. However in many cases the attacker may not have physical access to the site, so he or she will use a rogue AP as part of a more sophisticated attack.

In this case, an attacker would set up a rogue AP outside the building in an attempt to lure a client into mistakenly associating with it. When this happens, the attacker is free to obtain data from that client directly and can also gain information such as the client's login info and credentials, which the attacker could use at a later time (Fig. 2). While the focus thus far has been on access points, the same principles also apply to clients. A rogue client could indicate an unknown user trying to get unauthorized access to the network.

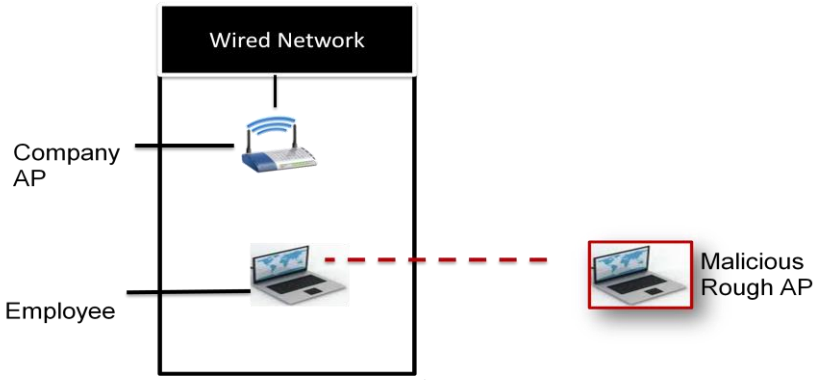

Fig. 2. Malicious rouge AP used to lure employees away from the enterprise network

On the other hand, it could be an unconfigured employee device searching randomly for any available connection. In either case it represents an issue that requires immediate attention from technical staff.

IV. ROGUE ACCESS POINTS SOLUTION

The solution to the issue of rogue devices will always begin with detection. Fundamentally, security staff needs to have complete visibility of every access point and client in the network coupled with clear-cut rules that identify the devices that are authorized to be in the network. The more specific the wireless policy, the easier rogue detection becomes. For example, if you know the MAC address of your devices, you can then easily identify rogues based on MAC address. In the same way, Rogues can also be identified based on other factors such as the hardware vendor, Channel, or SSID.

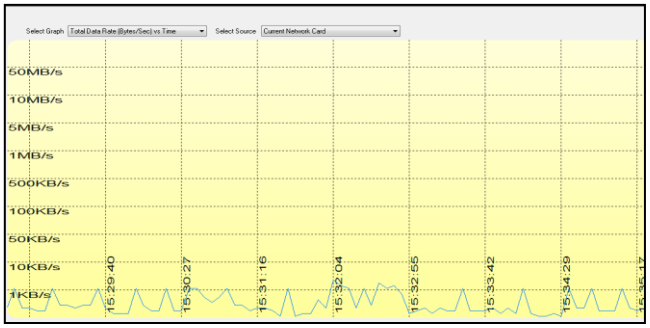

Fig. 3 The total data receives from rogue access point [7]

All of this requires the ability to scan the airwaves and identify each device based on a variety of criteria, again illustrating the need for comprehensive wireless monitoring. As a closing note, it is important to think of rogue detection as part of the larger security policy and not the security policy itself. Rogue APs have been so well covered in the media that the tendency is to think of rogue detection and wireless security as the same thing. [10] This puts the cart before the horse in as much as it addresses the most publicized issue but ignores the hundreds of issues and weaknesses that sophisticated attackers would exploit.

A. ROGUE SUPPRESSION AND RESPONSE

Any rogue device should be considered a threat to the network and requires a set of responses on the part of network staff and security systems. The response process should ideally be broken to two phases—a suppression phase where the rogue device is immediately quarantined from the network, and a removal phase where the device is physically located by staff and potentially removed from the network.

- ROGUE SUPPRESSION:

When a rogue is detected, the first order of business is to limit its access to other wireless devices in your network and especially to the larger wired network. This can be done using blocking strategies that typically fall in one of two broad categories—wire side blocking and wireless blocking. Wire side blocking techniques seek to block rogues at the point they reach the wired network, namely at the port or the switch. This provides strong protection for the wired LAN and should be strongly considered as part of multi-layered approach to rogue suppression.

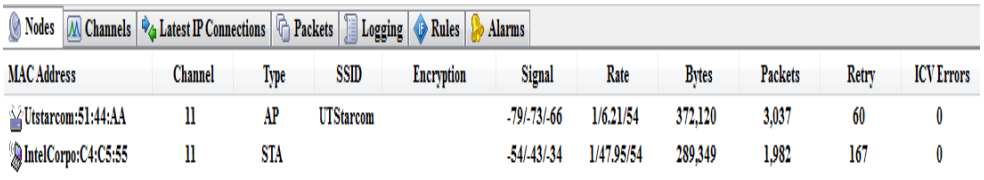

Fig.4 The available APs in the device range [7]

Wireless blocking involves the use of a separate wireless security device to block the rogue from making any connections on the wireless side. This is performed through a variety of methods, but the end goal is to insure that the device cannot make outbound connections to other devices and devices cannot make inbound connections to it. This ability to quarantine is of particular importance when you revisit the rogue scenarios discussed in the previous section. Recall that in many cases the

rogue may not even be plugged in to the wired LAN. [9] A malicious rogue user may attempt to lure clients to his AP as part of a larger attack on the network. Without the ability to block in the wireless domain, IT is essentially powerless to stop these attacks. Additionally, since wireless blocking suppresses the rogue at the source, it also provides additional protection to the wired network.

- PHYSICAL RESPONSE:

After a rogue device is quarantined a physical response to remove or reconfigure the device is still required. All blocking techniques, whether wired or wireless, will have some level of impact on the performance of the network. Shutting down a port obviously removes that port from use in the network, and is not a strategy that could be pursued indefinitely.

Wireless blocking requires the blocking device to regularly send blocking messages to the rogue device, which will result in the rogue repeatedly failing in its connection attempts. All of these messages constitute traffic on the WLAN that is essentially doing nothing in terms of the core function of the network, which is communication. While the effect of this process is negligible in individual cases, it does not make sense to incur this overhead on a large scale when the rogue can be removed. To remove a rogue device, IT will need to be able to locate it in space, and this will require specialized tools designed for the task. Such tools allow IT to lock in on a rogue's MAC address and track down the physical location of the device. This provides IT with the ability to pull the device out of the network and potentially meet its owner face-to-face. If the rogue has been brought in by an employee, you will want the opportunity to explain the security policy as well as get an understanding of the reasons why the user brought the device in the first place. Perhaps he or she has poor coverage from the corporate WLAN and was trying to solve a problem. From the above description the core of these solutions is the Wireless Intrusion Detection System (WIDS) that contains the analysis engine for this attack and other attacks. This engine automatically analyzes wireless network to proactively identify many threats. The WIDS enables wireless security beyond WEP, WPA by identifying vulnerabilities and attacks that cannot be protected simply by the use of encryption. By rapidly detecting these security holes, network operators can employ countermeasures using Wireless Intrusion Prevention System (WIPS) before intruders can do their damage. One such vulnerability that cannot be prevented with WEP is the presence of rogue wireless devices, including honeypot APs, where a hacker mimics a known AP to lure unsuspecting users. Once connected, the hacker can download a virus or steal confidential data. An example attack, which circumvents WEP, is WEPWedgie. This toolkit determines 802.11 WEP keystreams and injects traffic with Known keystreams. The Network Chemistry system the Wireless Intrusion Protection System [Network Chemistry] detects rogue devices, honeypot APs, and the use of WEPWedgie, among the many other vulnerabilities and intrusions it can detect. This tool is a very cost effective tool for small to medium businesses today. You can defend against intrusion and there are several products that can support this effort. The flagship product in the market today is CommView [7] and provides an IDS capability specifically for the Wi-Fi environment using an integrated system of sensors and a management console.

V. CONCLUSION

Security conscious enterprises are fortifying their wireless LANs with a layered approach to security that closely resembles the accepted security practices of wired networks. This layered approach addresses all network components by locking down the wireless LAN's perimeter, security communication across the wireless LAN and monitoring network traffic. The access points which have been deployed without the approval or against the organizations IT policy are very dangerous for network security. The proposed research describes rouge access point detection and suppression. The detected rouge access points can be suppressed by either wireless or wired blocking followed by physical response from network administration team. The proposed approach is further extendable by providing the built-in graphical positioning system support to find out the exact location of rogue access points.

References

1. Y. Fyodor, dSNORTNETT—A Distributed Intrusion Detection System, 2000 (June) (Available from: http://snortnet.scorpions.net/snortnet.pdf).
2. J. Viega, G. McGraw, Building Secure Software: How to Avoid Security Problems the Right Way, Addison Wesley, 2002.
3. G. Shipley, Chapter 12 bIntrusion Detection Systems (IDSs)Q, in: Shelley Johnston Markunday (Ed.), Maximum Security: A
4. Hacker's Guide To Protecting Your Internet Site And Network, third edition, Sams ublisher, Indiana, 2001.
5. R.A. Kemmerer, G. Vigna, Intrusion detection: a brief history and overview. Reliable Software Group, Computer Science Department, University of California Santa Barbara, Supplement to Computer Security and Privacy (2002) 27–30.
6. S.H. Oh, W.S. Lee, An anomaly intrusion detection method by clustering normal user behavior, Computers & Security 22 (7) (2003) 596–612.
7. CommView® for WiFi v.6.3, for capturing and analyzing network packets on wireless 802.11a/b/g/n networks (http://www.tamos.com/htmlhelp/commwifi/whatsnew.htm)
8. Char Sample and Kim Schaffer, Capitol College, "An Overview of Anomaly Detection" IT Pro January/February 2013 Publ ished by the IEEE C omputer S ociet y 1520-9202/13/$31.00 © 2013 IEEE
9. Kaixing Wu, Wei Zhang and Wenzeng Zhu, "A Study on the Application of Intrusion Detection Technology to WLAN" 978-1-61284-486-2/11/$26.00 ©2011 IEEE
10. ZHUO CHANG, YAN-LING ZHU, "The Design Of Wireless Intrusion Detection System Based On Immune Algorithm" 978-1-4577-0308-9/11/$26.00 ©2011 IEEE

AUTHOR(S) PROFILE

Mr. Ajay Patel, received the M.C.A and B.C.A degree in Computer Application from Ganpat University in 2006 and 2003, respectively. His Ph.D. in Computer Application is also on going. He is an assistant professor of faculty of computer application of Ganpat University in India. He is well interested in networking era. He has also work with data mining and gets enough expertise on data mining with wireless network. His ongoing research focused on intrusion detection in wireless LAN. He has published number of journal and conference papers in the area of his research interests. He is currently working on pattern matching and predication of wireless network traffic.

Dr. Ashok Patel, an eminent personality interested in finding ways to improve the teaching and learning process. The author has enormous research experience in the E-commerce and E-Governance. He has guided more the 15 Ph.D. students as well as Post Graduate level students in the diversified fields of computer application such as data mining, neural network, computer network, enterprise resources planning etc. He is a director of department of computer science of H. North Gujarat University of India. He is also working as a director in AICTE the apex body in India for technical education.

Ms. Hiral Patel, is an assistant professor of faculty of computer application of Ganpat University in India. She is starting to working on pattern matching and predication of financial data and wireless network traffic.

