

Implementing Honeypots as Part of a Simple Cost Effective Wireless Intrusion Detection System (April 2007)

H. M. Velupillai, R. P. van Heerden, and J. Vorster

Abstract—Wireless networks face innovative intrusion methods that have never been focused on wired networks. This paper describes a simple inexpensive way to implement a wireless intrusion detection system. The system takes advantage of the unique features of wireless networks to implement the wired network design of a honeypot. The paper also provides a script that allows the Atheros chipset to be modified to implement multiple wireless access points on one wireless card.

Index Terms—Computer Network Security, Data Security, Site Security Monitoring, Wireless LAN

I. INTRODUCTION

Wireless networks have been a miracle for organizations that don't have time to set up wired networks or simply cannot due to environmental, financial or physical constraints. Temporary offices have now become possible. Companies have reported large savings from not having to install wired networks. These savings come at the price of security. It is no longer necessary for an attacker to bypass firewalls on a wired network to get onto an organisation's network. Nor does he have to evade physical barriers. An attacker can now be sitting in the coffee shop across the road and be on the organisation's network.

More frightening is when employees set up unauthorized wireless networks that are connected to the wired network. Due to the ease with which wireless network can be set up the employees can easily set them up for valid reasons. However the reason that wireless networks are so easy to set up is that they come with a lot of default settings. These default settings are usually known to attackers.

The new practice of warflying enables attackers to quickly identify all the wireless networks in an area [1].

H. M. Velupillai is a Researcher at the Council for Scientific and Industrial Research (CSIR) in Pretoria, South Africa (phone: 012 841 3931 fax: 012 841 5025 email: hvelupillai@csir.co.za).

R. P. van Heerden is a Researcher at the Council for Scientific and Industrial Research (CSIR) in Pretoria, South Africa (phone: 012 841 3931 fax: 012 841 5025 email: rvheerden@csir.co.za).

J. Vorster is a Research Group Leader at the Council for Scientific and Industrial Research (CSIR) in Pretoria, South Africa (phone: 012 841 2258 fax: 012 841 5025 email: jvorster@csir.co.za).

This paper was funded by the Parliamentary Grant.

The first step in stopping intrusions is knowing when they are happening. More importantly it is important to get advanced warning of a possible intrusion. There have been several previous proposals for using the methods described in this paper [2]. This paper however takes into consideration the advances in wireless security and vulnerabilities to provide a simple method of implementing a WIDS on a small scale.

II. BACKGROUND

A brief background of threats faced by the 802.11 protocol is covered in this section. Methods that can be used to detect and mitigate these threats are also provided.

A. Wardriving

Wardriving is an activity that is nearly as old as wireless networks. Attackers set up a wireless sniffer in a car and then drive around trying to pickup wireless networks [3]. The major problem with this activity is that these attackers usually publish their captured data on the internet [4]. This allows others to use the data. Wardriving will be discussed on more detail later in this report. It is generally agreed that Peter Shipley invented wardriving [5], [6].

Depending on the knowledge and equipment available to the hacker wardriving can be done either with a great deal of stealth or not.

The end point is that the hacker will connect to the access point with the least security settings.

B. Honeypots

Honey pots are devices that were designed to be used on wired networks. The idea was that the honeypot would have a lower security protection than the rest of the machines on the network. A potential hacker would then target the honey pot first since it would be the easiest machine to compromise. There are various methods of monitoring a honeypot. The goal is to know when and how a machine was compromised. This would give an indication that an intruder is present on the network as well as his level of skill.

C. Fake Access Points

The idea of fake access points was first developed by a wireless hacking group called Black Alchemy [7]. They created a Perl script that created thousands of fake access points that only exist for a small amount of time. It was therefore not possible for a hacker to make any connections

to these access points. In essence the script created chaff to hide the real access point.

The flaw in this method is that if a hacker monitored a given location near the real access point for a long period of time he would be able to determine that the real access point. The real access point would be the only access point that continually appeared on all his scans.

D. Wireless Intrusion Detection System

This paper describes how to integrate the concepts of fake access points and honeypots. The Atheros chipset allows a user to do several modifications.

Using the Atheros chipset it is possible to set up one network card to pretend to be several access points. More importantly it is possible for connections to be made to each of the access points. For ease of reading the access points created by the wireless honeypot will be called fake access points from now on to differentiate them from legitimate access points. However they still accept connections made to them.

The Wireless Intrusion Detection System (WIDS) will monitor the wireless spectrum. The goal of the Wireless IDS is to detect nodes that connect to several fake access points.

This paper describes a two stage framework for the establishment of a wireless honeypot.

III. DESIGN

The wireless honeypot has only one requirement, to identify potential hackers. Identifying the physical hackers may not be possible and is very difficult so we will settle for identifying the Media Access Control (MAC) address of the network cards the hackers are using.

Fig 1 shows a high level view of what the wireless honeypot system would look like. A real access point exists. This access point will connect to the organisation's network. A machine will also be set up to run the Wireless IDS. The wireless honeypot machine will be set up as shown on the figure. The wireless honeypot will be assigned a valid Internet Protocol (IP) address. However it will have no connection to any other network.

The wireless honeypot can generate more any number of access points. The idea is to create a number of fake access points that will no seem suspicious. This means that if the area the Wireless IDS is to be deployed in contains roughly N access points including the access point deployed by your organization. Deploying up to N/2 fake access points over a month will not raise a lot of eyebrows.

A. Naming Conventions

Each access point has a Service Set Identifier (SSID). The fake access points should have SSID names that are not related. The names should also not be related with any of the SSID names for legitimate access points that occur near the Wireless IDS. This will prevent legitimate users connecting to a fake access point by mistake.

B. Security Protocol

The wireless honeypot can implement different security

protocols on each fake access point. This means that the access points can be configured with variant security protocols. The only clear guideline is that the access point security level must be below or equal to that of the real access point. Wireless security has evolved from none existent to a highly sophisticated security implementation system.

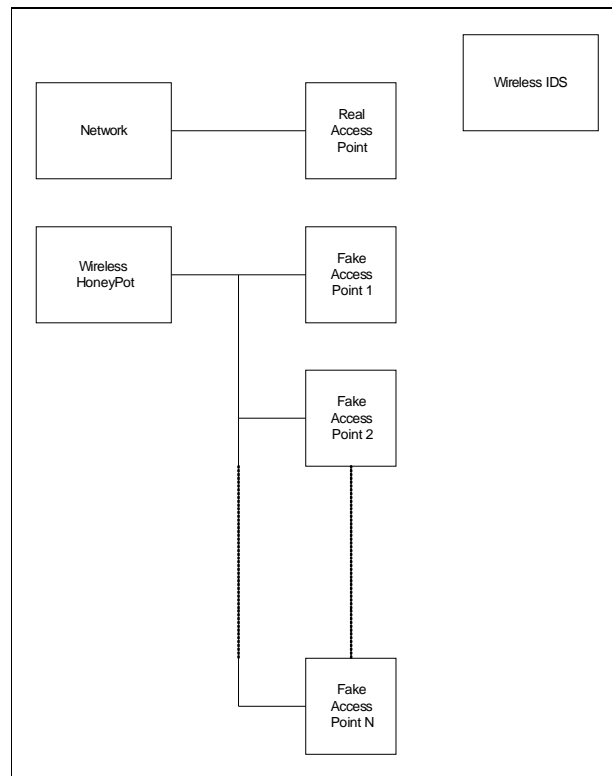


Fig. 1. Wireless Honeypot Setup.

C. Wired Equivalent Privacy

The first security protocol Wired Equivalent Privacy (WEP) was released in 1999. The WEP security protocol is based on the Rivest Cipher 4 (RC4) encryption standard with a secret key of 40 or 104 bits. The advertised number of 64 and 128 bits is misleading, only 40 or 104 bits are used for encryption [8]. The remaining 24 bits are used as the Initialisation Vector (IV) to encrypt the message. The IV is the key to WEP security and the 802.11 standard does not specify a correct usage of IVs, leaving the WEP security system fundamentally flawed [9]-[11]. The first solution to the fundamental WEP security problems was to increase the size of the WEP key, but as shown by J. Walker [12] increasing the key size does not solve any of WEP's security problems.

D. Wi-Fi Protected Access

In 2003 the Wi-Fi Alliance released a security protocol Wi-Fi Protected Access (WPA). WPA solved the IV problem by randomly generating IV's and using a shared secret key known as a Pre-Shared Key (PSK) to generate a pseudo-random keystream equal to the 802.11 frame payload [10]. The WPA vulnerability is an attack against

the secret key. The mechanism to exchange the PSK is transmitted by the Temporal Key Integrity Protocol (TKIP). The TKIP can be recorded by a passive listening station and then attacked with a brute force or dictionary list attack.

E. WPA2

WPA2 was designed according to the 802.11i standard (the 802.11i standard was never commercially used). WPA2 will be included in the 802.11n standard. The WPA2 security protocol utilizes the Advanced Encryption Standard (AES) encryption. WPA2 replaced TKIP with Counter mode CBC MAC Protocol (CCMP). CCMP rotates the encryption keys and uses message integrity checks [13], [14]. At the time of writing WPA2 has no publicly known vulnerabilities.

F. MAC

MAC addresses can also be used for security. Every network device has a unique MAC address. Most access points can be set up to limit network access to devices with a specific MAC address. These MAC addresses are not concealed and can easily be spoofed.

G. Physically Locating Wireless Hackers

Wireless hackers unlike wired hackers have to be close to their target access point. This allows them to be apprehended [15]. Physically locating wireless hackers is beyond the scope of this paper.

IV. IMPLEMENTATION

A wireless network has been set up. This network must be protected from intruders. There is only one access point that allows access to the wireless network. The primary existence of the wireless network is to provide access to the wired network. The access point has the WPA security protocol implemented. A firewall has been setup between the access point and the rest of organisation's network. The firewall allows all communication through, the only exception is if the IP or MAC address of one of the communication partners is placed on the firewalls blocklist. In this case the communication is blocked.

Preliminary scans indicate that there are around 23 access points found within scanning range of the test sites. Using different types of antennas gave different values.

It was decided to use the results from the long range antennas since these are the ones used by the best equipped wardrivers. Based on this value it was decided to use ten fake access points.

The real access points that the system must protect employ WPA. This allowed the fake access points to implement both WEP and WPA. No access points were set up with MAC address filtering since this method can be easily broken.

To break this method however requires a constant monitoring of the nodes that connect to the access point. Since we don't want hackers looking too closely at the nodes that connect to the fake access points MAC address filtering was not implemented.

A. SSID

The following names were chosen:

- NID, No security Protocols.
- CES, WEP implemented.
- Pierre, WPA implemented.
- Cina, WEP implemented.
- Kepyrt, WEP implemented.
- Metric, WEP implemented.
- Asterix, WPA implemented.
- June, No security Protocols.
- Wadmin, No security Protocols.
- Sams, No security Protocols.

The names do not stand out among the rest of the legitimate access points nor do they closely resemble any of the legitimate access point. Any one who tries and connects to these fake access points can be reasonably counted as a potential intruder. The Appendix contains the commands that were used to create these fake access points.

B. Monitoring

The open source program Airodump which is part of the Aircrack suite of tools was used to monitor the wireless spectrum [16]. The program was configured to record all the MAC addresses that connect to the ten specific access points. These captured MAC addresses can then be added to the blocklist of the firewall that protects the legitimate access point.

The firewall blocklist is updated daily. There is no network connection between the firewall and the fake access points. The blocklist will have to be updated manually. This division prevents a hacker who compromises the fake access points from having access to the firewall.

V. CONCLUSION

Wireless networks have allowed savings in time and money as they replace the need to install wired networks. Wireless networks however remove the need for an attacker to be physically connected to the network.

There are other tools that allow administrators to detect the presence of hackers. However these tools are usually commercial. The goal of this paper is to present a design of a cheap easy to implement method that can be used by anyone who can setup a wireless network.

The second goal is to move into using the knowledge gained implementing honeypots on wired networks to implement honeypots on wireless networks. Wireless networks have numerous advantages and disadvantages when compared to wired networks. Hackers already know all the disadvantages. This framework attempts to use the advantages of wireless networks against them.

APPENDIX

The following commands were used to create two wireless network access points (Note, athX may differ if more than one Atheros card has been used):

```
#pccardctl insert
```

```
#wlanconfig ath0 destroy
#ifconfig wifi0 up
#ifconfig wifi0 down
#wlanconfig ath10 create wlandev wifi0 wlanmode ap
#ifconfig ath10 channel 1
#ifconfig ath10 essid NID
#ifconfig ath10 up
#wlanconfig ath11 create wlandev wifi0 wlanmode ap
#ifconfig ath11 channel 1
#ifconfig ath11 essid CES
#ifconfig ath11 up
```

The above commands can be replicated to create all ten access points.

REFERENCES

- [1] E. Lawrence, and J. Lawrence, "Threats to the mobile enterprise: jurisprudence analysis of wardriving and warchalking," in *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04)*, pp. 268 – 273, 2004.
- [2] S. Yek, "Implementing network defence using deception in a wireless honeypot," in *Proceedings of the 2nd Australian Computer Conference on Information and Network Forensics*, pp. 2-15, 2004.
- [3] WarDriving. <http://www.wardriving.com>. Last accessed 10 April 2007.
- [4] P. Geo. <http://www.perrygeo.net/wordpress>. Last accessed 10 April 2007.
- [5] Open WLANs - The early years of WarDriving - Peter Shipley, <http://www.dis.org/filez/openlans.pdf>. Last accessed 10 April 2007.
- [6] G. Tagg, Wireless LANs- the threat to Network and how to address them, in *Proceedings of the 3rd International Information Security Conference & Workshop (Cyprus Infosec)*, 2003.
- [7] Black Alchemy. <http://www.blackalchemy.to/project/fakeap/>. Last accessed 10 April 2007.
- [8] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: the Insecurity of 802.11," in *Proceedings of the 7th Annual international Conference on Mobile Computing and Networking (MobiCom '01)*, 2001, pp. 180-189, 2001.
- [9] S. Wong, "The Evolution of wireless Security in 802.11 networks: WEP, WPA and 802.11 standards," SANS Institute white paper, 2003.
- [10] W.A. Arbaugh, N. Shankar, and Y.J. Wan, "Your 802.11 Wireless Network has No Clothes," in *Proceedings of the IEEE International Conference on Wireless LANs and Home Networks*, pp. 44-51, 2002.
- [11] A. Stubblefiend, J. Ioannidis, and A.D. Rubin, "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP," in *Proceedings of the 9th Network and Distributed System Security Symposium (NDSS'02)*, pp. 6-8, 2002.
- [12] J.R. Walker, "Unsafe at any key size: An analysis of WEP encapsulation," Technical Report 03628E IEEE Standards 802.11 Committee, 2000.
- [13] K. Lee, H. Kim, and J. Song, "Lightweight packet authentication in IEEE 802.11," in *Proceedings of the*

Wireless Telecommunications Symposium (WTS'05), pp. 268 – 273, 2005.

- [14] A. Wool, "A note on the fragility of the "Michael" message integrity code," *IEEE Transactions on Wireless Communications*, Vol. 3, Issue 5, pp. 1459-1462, 2004.
- [15] F. Adelstein, P. Alla, R. Joyce, G.G. Richards, "Physically Locating Wireless Intruders," in *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04)*, pp. 482, 2004.
- [16] Aircrack-ng. <http://www.aircrack-ng.org>. Last accessed 27 March 2007.

Harry M. Velupillai received his B.Eng Hons (Computer Engineering, 2004) degree from the University of Pretoria. He is currently working as a researcher at the CSIR.

Renier P. van Heerden received his M.Eng (Computer Engineering, 2002) degree from the University of Pretoria. He is currently working as a senior researcher at the CSIR.

Johannes Vorster received his B.Sc Hons (Computer Science, 1992) degree from the University of Pretoria. He is currently working as a research group leader at the CSIR.