https://doi.org/10.48009/1_iis_2012_209-214
Issues in Information Systems
Volume 13, Issue 1, pp. 209-214, 2012

A COMPARISON OF WIRELESS SECURITY PROCEDURES: SECURITY COUPLED WITH EASE OF IMPLEMENTATION FOR A COLLEGE CAMPUS

Ronrico D. Slack, Georgia College & State University, ronrico.slack@bobcats.gcsu.edu
Bryan Marshall, Georgia College & State University, bryan.marshall@gcsu.edu

ABSTRACT

Currently wireless networks are virtually everywhere and though security is easily configurable some people opt to leave their wireless networks unsecured. There are many blogs and columns available online as to what security measure is the best to implement and when, however very few articles actually compare and contrast methods side by side. In this paper we hope to accomplish just by researching the pros and cons of each method and proposing which method should be implemented depending on the situation. Based on your needs the victor from comparison was WPA2 Enterprise, hence we built a RADIUS server and attempted to integrate it into this newly secured network. We then utilized a Microsoft Windows 7 laptop to attempt to connect to the network. Then finally we tested each security measure's effect on performance due to the different methods of encryption. We found that RADIUS servers are somewhat complex to setup and integrate with WPA2 Enterprise, hence we propose the use of WPA2 Personal with AES encryption; the second most secure method that does not hamper performance and is relatively simple to configure and implement. Therefore, this research lends itself to verifying what was found on the blog sites and columns as to which method offers the best security while remaining simple to set up.

Keywords: Wireless, Security, College Campus, Comparison,

INTRODUCTION

In today's world, data is transferred in many mediums. These range from the very basic LAN (Local Area Network) in which data is shared among computers /systems in very small wired environment, scaling up to the colossal WAN (Wide Area Network) spanning in essence, the world. An example of the implementation of a WAN is the internet.

However, this paper is focused on the very basic LAN, more so the WLAN (Wireless Local Area Network); A modification to the LAN, which allows data to be transferred among systems on the LAN wirelessly. The WLAN's inception came about in 1979 but it was not until 1996 onwards that the WLAN gained popularity and was now relatively inexpensive. It is because of its pricing in the early stages that businesses were the primary users of WLAN's.

As it stands today, WLAN's are not restricted to organizations and business; they can be personalized and implemented in schools and even in the home. Most colleges have a wireless network (WLAN) in place to facilitate their students in connecting to resources. Some colleges have their wireless secured while others remain unsecured. The campus which inspired this paper has a wireless network implemented and is currently unsecured; however, they wish to have it secured. The purpose of this paper is to determine the most efficient way to secure GCSU's WLAN.

LITERATURE REVIEW

Since its emergence, WLAN's (Wireless Local Area Networks) have been a blessing and sometimes a curse. Early wireless networks lacked security until the inception of WEP (Wireless Equivalency Privacy), which offered some comfort to users. If data content was void of sensitive information, such as identities, email addresses, street addresses, and social security numbers, WEP was an ideal level of security [1]. This however was short lived as the encryption used by WEP was discovered to be easily cracked [2]. In an effort to bolster security, one would increase

the length and complexity of the pre-shared key. This would slow the hacker's progress in compromising the network, but not stop them.

Luckily, routers offered added features to help secure the wireless network. This came in the form of MAC-Address filtering, which when implemented, would improve the security of a WLAN. Anyone can get obtain all the credentials to access the network such as SSID (Service Set Identifier) and encryption keys; however, when MAC Address filtering is enabled, the router performs an additional test before access to the network is granted. Thus, the increased verifications will limit the likelihood of unauthorized network access [7]. Sadly, MAC Address filtering also falls short of its intended purpose. All a would-be hacker needs to do is sniff the packets being transmitted between a legitimate user and the company. Once the legitimate user's MAC Address is determined, the hacker simply copies it and uses it as his/her MAC Address and thus they have access to the network [9].
Adding to the list of bonus features there is the option to hide the SSID (Server Set Identifier). The premise is, if a SSID is hidden it should be more difficult to be attacked. This sounds feasible, however, like MAC Address filtering hackers have a work around to unravel this option in wireless security. Furthermore, software is readily available online to help one achieve this task of finding hidden SSID's [8]. Thus hiding your SSID only sounds effective, but in reality, it really is a waste of energy and time.

After realizing the weakness in WEP, Cisco introduced the world to LEAP (Lightweight Extensible Authentication Protocol) which would overcome the shortcomings of WEP, and so it did for a time. LEAP's design gave intruders/hackers two rewards for the cost of one. Reason being, LEAP authentication credentials usually allow access to the wireless network and are usually user's actual login credentials. Thus, LEAP was probably a worse security measure than what it was intended to best, WEP [10].

Focusing on the previous failures to adequately secure wireless networks, WPA (Wi-Fi Protected Access) was introduced to ease our woes. WPA featured a much stronger encryption algorithm and unlike WEP, WPA continuously changes the encryption key each time a packet is transmitted to increase security [5]. WPA offered two ways of application, pre-shared key which was previously offered by WEP and newly introduced, Enterprise. In Enterprise, users must obtain authentication from a RADIUS (Remote Authentication Dial In User Service) server before it can access the network. WPA would appear to be the answer we have been waiting for until, once again vulnerabilities were discovered. WPA was found to share the same key management vulnerabilities that its predecessor WEP experienced in its glory days. Further to that, WPA has another vulnerability when undergoing its 4-way handshake during authentication. It has been discovered that a brute force attack at this point in time could compromise the integrity of the exchange, thus your key can be discovered by a hacker [11]. After revisiting the drawing board, Wi-Fi Alliance introduced WPA2, a second generation to the recently partially failed WPA. The major upgrade came in the form of the encryption method used. WPA2 now boasts AES (Advanced Encryption Standard), which is much more potent than WPA's TKIP(Temporal Integrity Key Protocol). TKIP was replaced because it was susceptible to being cracked, whereas AES is extremely difficult to crack [6]. Sadly, nothing is perfect, thus WPA2 has vulnerability. Though it is a flaw, this vulnerability can only be exploited by an authenticated user which would normally be an employee, thus there should not be a real issue in using WPA2 [4].

CONSTRUCTS

Based on finding of the three technologies, WEP, WPA, and WPA2, we have decided to implement WPA2 Enterprise using AES encryption. As stated earlier in the paper, AES is the most robust encryption available to date. Couple this encryption with the authentication offered by Enterprise; the WLAN should be relatively unbreakable. Enterprise applications however require connection to an authentication server in the form of RADIUS or LDAP in order to function. Hypothetically speaking, a radius server should be relatively easy to set up and integrate with this application of WPA2 Enterprise.

Q1. How simple is it to create and manage a RADIUS Server?

Before implementation of new technologies, compatibility for the existing infrastructure is always a concern and this time is now different. Based on unobtrusive observations it appears that the existing infrastructure, in this case laptops, fall between two operating systems, Windows 7 and Apple. With this knowledge, we hypothesize that both systems will be compatible with the application of WPA2 Enterprise using AES encryption.

Q2. Are Windows and Apple operating systems completely compatible with WPA2 Enterprise?

Continuing, the algorithms that make AES work is processor and memory intensive on both ends of the WLAN connection. Thus, every bit being transferred will be encrypted using AES, users on this WPA2 Enterprise network may experience slower data rates. Thus, we hypothesize that although AES will indeed make the network unbreakable, it may also hamper performance.

Q3. Will the utilization of AES encryption hamper the performance of the wireless system?

Based on what is questioned and hypothesized, a determination can be made as to what it takes to create and manage a RADIUS server while integrating it with a WLAN secured by the enterprise method. We will also verify compatibility across operating systems and demystify the perception of higher encryption will in turn yield lower performance for more security.

METHOD OF TESTING

To test the first proposed hypothesis we built a controlled environment in which a test radius server was set up and a windows based operating system laptop was used to connect and authenticate against this radius server using RADIUS test software. This test was carried out on a wired network, hence systems, laptop and RADIUS server, need were on the same subnet connected by Ethernet cables. The specifications for the stated equipment necessary are stated below:

The Windows 7 laptop utilized had the following specifications:

- 2 GHz dual core processor
- 4 GB RAM
- 64 bit Windows 7
- Realtek PCIe FE Family Controller
- NTRadPing 1.5

The RADIUS Server utilized had the following specifications:

- LINUX UBUNTU Server 10.04
- 2 GHz dual core processor
- 2GB RAM
- Freeradiusserver

After the above test was completed and the RADIUS server is up and running, a Windows 7 Laptop was introduced into the test environment illustrated above. The laptop attempted to connect to a wireless access point that is unsecured. Once the connection was verified, the wireless access point was secured with WPA2 Enterprise utilizing AES encryption. The authentication server of the wireless access point was the test radius server spoken of earlier. The Windows laptop then attempted to connect to the newly secured network.

The equipment required for this next test is as follows:

Windows laptop utilized had the following specifications:

- 2.3 GHz dual core AMD Turion processor
- 4 GB RAM

- 64 bit Windows 7
- Realtek RTL8191SE Wireless LAN 802.11n PCI-E NIC

The Wireless access point used and the RADIUS server used are stated below:

- Cisco Aironet 1100 AG Series

The RADIUS Server utilized had the following specifications:

- LINUX UBUNTU Server 10.04
- 2 GHz dual core processor
- 2GB RAM
- Freeradiusserver

Finally, we tested the performance of our newly secured network. Both systems, Windows 7 and and a newly introduced Apple laptop, connected to the WLAN using different security schemes. These schemes ranged from an open network to WEP, with all its available encryption methods, up to WPA2 Personal utilizing AES encryption. After connecting, ping tests were carried out and results were recorded, then results were compared and contrasted. The ping was utilized because it displays the roundtrip (the time taken for the packet to reach the ping destination and return) of a packet, thus if encryption was to hamper performance it would be apparent in this simple test.

The Apple laptop utilized had the following specifications:

- 2.2GHz or 2.4GHz quad-core Intel Core i7 processor with 6MB shared L3 cache
- 4GB (two 2GB SO-DIMMs) of 1333MHz DDR3 memory;
- OS X Lion
- AirPort Extreme

Results

Building and configuring the RADIUS server was not a difficult venture. In the beginning when dealing with simple authentication, all initial tests using NTRadPing yielded success. However, when it came time to integrate it with the implementation of WPA2 Enterprise we found that the laptop utilized PEAP authentication and the RADIUS server utilized MD5, hence we were never able to authenticate. Therefore, the hypothesis is confirmed to be false, it is not easy to set up and integrate a RADIUS Server.

Enterprise compatibility with Windows and Apple was not verified as the prerequisite test failed miserably, which was to get the Windows laptop to authenticate and access the WPA2 Enterprise network. Hence, the hypothesis of compatibility with Microsoft and Apple with regards to WPA2 Enterprise is unconfirmed.

Using the various encryption methods, the results of performance were tabulated and are displayed below:

The Windows laptop yielded:

Table 1. Windows Pingtest

Security Options	Test 1 (ms)		Test 2 (ms)		Test 3 (ms)	
	Ping	Jitter	Ping	Jitter	Ping	Jitter
Open	49	3	49	5	47	1
WEP 40bit	48	1	49	3	49	6
WEP 128bit	49	5	48	2	49	5
WPA Personal	48	3	48	1	48	1
WPA2 Personal	49	4	47	1	48	2

The Apple Laptop yielded:

Table 2. Apple Pingtest

Security Options	Test 1 (ms)		Test 2 (ms)		Test 3 (ms)	
	Ping	Jitter	Ping	Jitter	Ping	Jitter
Open	67	2	66	2	67	2
WEP 40bit	68	4	67	1	67	1
WEP 128bit	67	1	67	1	67	2
WPA Personal	67	1	67	1	67	1
WPA2 Personal	68	4	67	2	67	2

Based on the results in both tables, almost all security methods yielded similar results; thus, there is barely any noticeable difference in performance when security measures such as WPA2 Personal using AES encryption is implemented. Therefore, I strongly propose the implementation of WPA2 Personal. Going further, students mostly use the WLAN to do research for class and connect to social networking sites, things that will not suffer from a slightly longer ping rate if any. Thus, the hypothesis that WPA2 Personal utilizing AES encryption will hamper performance is confirmed to be false.

CONCLUSION

This study lends credibility to the claim that WPA2 Personal with AES encryption is the best wireless security measure to date. The only flaw discovered will only be a threat if there are attacks from inside the network, meaning an employee were to assault the network. Other than that, it is virtually impossible to gain access to this network without using the proper channel.

Going further, we see that no security measure impedes performance substantially if at all. Therefore any security measure could have been used, but due to the nature of data that traverses the network and the simplicity of setting up such security, we propose the implementation of the strongest, WPA2 Personal with AES encryption.

Finally, we see that both dominant operating systems used on campus have no compatibility issues with WPA2 Personal, thus implementation should be no problem. We only propose that students and staff carry their end devices to the IT section of the campus to get it set up to access the network, meaning, no student or staff outside of IT

working on this project should know the password. This will almost ensure that the vulnerability found in WPA2 is not exploited since everyone at the campus signed an honor code.

VALIDITY CONCERNS

The RADIUS Server was configured on LINUX UBUNTU Server 10.04 to accommodate one (1) user, thus this is not a true representation when implementing this system to cater to thousands of users. We are unaware of the maximum number of users the RADIUS Server can facilitate before it starts to experience difficulty in authenticating users.

These tests were only conducted with the two operating systems stated above; there may be other operating systems and different configurations than the ones above on campus. Some systems may have less RAM than that used in the test, some may have a different wireless card than that stated above.

This experiment was conducted at Georgia College & State University and may not be a true representation of wireless access points used at all tertiary level institutions. Each access point can host a specific number of users, though it may not merely be one user, it is doubtable one access point can host over 1000 users at one time. Further to that, utilizing AES encryption, the amount of users accommodated my decrease due to processing power of the access point.

This enterprise experiment was conducted with MD5 as the authentication method and the use of certificates were disregarded, therefore configuring the server to utilize certificates may yield a different result. Furthermore the laptop used to test authentication only utilized PEAP, thus, if a laptop that utilizes MD5 for authentication was used a different result may be yielded.

REFERENCES

1. Bloomquist, Jane; Musa, Atif (2004*), "Secure your wireless network"*, Trade Journals, Vol. 24, Issue No. 9, pp. 20,22,24
2. Breeding, Marshall (2005), *"Wireless Network Configuration and Security Strategies."*, Library Technology Reports; Sep/Oct2005, Vol. 41 Issue 5, p21-30, 10p
3. Breeding, M. (2005). "*Implementing Wireless Networks Without Compromising Security"*. Computers In Libraries, 25(3), 31-33
4. Caro, I. (2010). "*Is my private WLAN secure - Vulnerability in WPA2 protocol (Hole 196)?"*. Retrieved January 14, 2012, from http://labs.swisscom.ch/it/content/my-private-wlan-secure-vulnerability-wpa2-protocol-hole-196
5. Hruska, J. (2009*). "The ABCs of securing your wireless network*." Retrieved January 14, 2012, from http://arstechnica.com/security/news/2008/04/wireless-security.ars
6. Katz, F. H. (n.d). "*WPA vs. WPA2: Is WPA2 Really an Improvement on WPA?*." Retrieved January 14, 2012, from http://infotech.armstrong.edu/katz/katz/Frank_Katz_CSC2010.pdf
7. Mitchell, B. (n.d). "*Enable MAC Address Filtering on Wireless Access Points and Routers"*. Retrieved January 14, 2012, from http://compnetworking.about.com/cs/wirelessproducts/qt/macaddress.htm
8. (n.d). Retrieved January 14, 2012, from http://www.howtogeek.com/howto/28653/debunking-myths-is-hiding-your-wireless-ssid-really-more-secure/
9. Ou, G. (2005). "*The six dumbest ways to secure a wireless LAN*." Retrieved January 14, 2012, from http://www.zdnet.com/blog/ou/the-six-dumbest-ways-to-secure-a-wireless-lan/43
10. Ou, G. (2007). "*Ultimate wireless security guide: An introduction to LEAP authentication"*. Retrieved January 14, 2012, from http://www.techrepublic.com/article/ultimate-wireless-security-guide-an-introduction-to-leap-authentication/6148551
11. Padilla, Daniel; Guillen, Edward (2005*), "Weaknesses and Strengths Analysis over Wireless Network Security Standards."*, World Academy of Science, Engineering & Technology; Feb2011, Vol. 72, p515-520
12. (2012) Internet. Retrieved March 27, 2012 from http://en.wikipedia.org/wiki/Metropolitan_area_network
13. (2012) Internet. Retrieved March 27, 2012 from http://en.wikipedia.org/wiki/Wireless_LAN