Global Information Assurance Certification Paper

Wireless Security: Past, Present and Future

Keith Morris

GIAC Security Essentials Certification (GSEC)

Version 1.4b
Option 1

September 12, 2003

Table of Contents

Abstract

This is a look at the state of wireless security. We will look at where it was when it was first introduced; where it is today; and the direction wireless security is headed in. When first introduced wireless security was weak and easily broken. Today it is more secure thanks to new technology. The future of wireless security is a robust system which will provide state of the art protection, and deter most if not all attacks, providing peace of mind to the end user.

Introduction

Throughout this paper I will be developing an analogy between the security a user has deployed in his wireless network and the security a home owner has deployed in his home. This is intended to give a non technical reader of this paper an idea of the state of wireless security available in a manner the reader can easily understand. At the end of each section we will compare the highest level of security available for a wireless network user with the equivalent amount of home security the user would have installed.

A Look at the Past

When Wireless technology was first introduced, the wireless routers default state was to disable encryption and broadcast the service set identifier (SSID) in the open. This meant anyone with a wireless network card installed and who was within proximity of your wireless local area network (LAN) could find and connect to your network. Since many of the computer operating systems are wide open and accessible in a default installation, this often meant that access to your network through your wireless LAN gave the intruder full access to your computer as well. This early state was the equivalent of leaving your front door wide open in your house and having no alarm installed. Anyone could come walking in from the honest but curious neighbor to a criminal who wants to rob you or worse.

One of the basic security steps the user could take would be to set the router to not broadcast the SSID. In addition to this, the user would have to change the SSID from its default value to something only known to the user preferably. This made the hackers job of penetrating your wireless network more difficult, because he would have to guess your SSID in order to connect to your network. In addition to this, you would want to enable encryption. A simple idea not often employed is locating the access point (wireless router) in the middle of the room, apartment or building in which it is being deployed. This will minimize the signal available outside the deployed area which can be used to break in and will also maximize the signal where it is supposed to be being used. One other step available to users at this point in time is limiting your network to just the MAC addresses of the wireless network cards you will use to connect to the wireless

access point. While none of these actions themselves will make you secure, all of them together will help to maximize your wireless network's security.

There are additional steps available, but many of these steps would be considered only by businesses or government agencies requiring an even higher level of assurance that no one is penetrating or eavesdropping on their network. These steps are expensive and involve physical changes to the building to block the signals from leaving the building. For instance, the walls could be lined and shielded to block all radio frequencies from entering or leaving. Signal jammers could be deployed. Having building set back a good distance from the road with protected perimeters from the land helps keep people from being able to communicate with your wireless network without being authorized. These are just a few examples of physical security that can be taken in additional to the configuration, authentication and configuration of the wireless network to provide defense in depth to their computer systems.

This brings us to a discussion of the only encryption technology available to wireless networking at the time: WEP.

Wireless Encryption Protocol

In the early days, the only encryption available to the users of wireless technology was wireless encryption protocol (WEP). WEP uses a single static 40 bit or 128 bit key for encryption. A quick search of the web will turn up many tools available to crack this protocol. There are many different types of attacks available against WEP. These include passive attacks to decrypt traffic, active attacks to inject traffic, active attacks to decrypt traffic, table based attacks and monitoring encrypted traffic. For a detailed analysis of WEP's weaknesses and the available attacks, see the article "Security of the WEP algorithm". [3]

These various attack types are designed to attack the numerous vulnerabilities known to be inherent in WEP. Internet Security Systems provides a thorough discussion of the vulnerabilities as shown:

> Although attacks against 802.11b and other wireless technologies will undoubtedly increase in number and sophistication over time, most current 802.11b risks fall into seven basic categories:
>
> - Insertion attacks
> - Interception and unauthorized monitoring of wireless traffic
> - Jamming
> - Client-to-Client attacks
> - Brute force attacks against access point passwords
> - Encryption attacks
> - Misconfigurations

Note that these classifications can apply to any wireless technology, not just 802.11b. [11]

When implementing our wireless network, we need to take steps to prevent these vulnerabilities from being exploited. This is true for hardware using WEP, WPA, WPA2 or any other protection scheme which might come along.

To implement WEP on your wireless network you would generate a key on your router. This key could be either 40 bits or 128 bits if your hardware supported it. You would then have to enter that key into all your wireless network cards, in order for them to be able to communicate with your router. This can be very cumbersome if you are implementing a large wireless network such as in a medium or large business.

Another problem implementing WEP is that vendors have not come up with a standard way of entering the WEP data. Some vendors require a hexadecimal value while others use an ASCII string for the pass phrase and most of the software for entering this value does not identify what is required in the field. Therefore trying to get wireless cards from one vendor to work with wireless access points (wireless routers) from another vendor can be very difficult or impossible. Enabling WEP on your wireless network can also cause a performance hit on your network. Tim Higgins backs this up with his statement, "Add in the fact that some wireless products suffer a WEP-enabled **throughput reduction** of up to 50%, and you can see why WEP has such a bad reputation." [6]

Now that we have implemented WEP on our network and stop broadcasting our SSID to anyone listening, we have taken the first steps to securing our wireless network. In continuing our earlier analogy, we have now locked the front door to our house. We have installed an alarm system which is not monitored and has an easily guessed code. At this point we are keeping the honest neighbors out of the house, but are still easily accessible to the professional criminal with a minimum amount of effort on his part.

Taking Stop Gap Measures

A large number of wireless networks are deployed in the field with only WEP as security. Given the many known weaknesses of WEP, something is needed to improve security in our deployed networks while we are waiting for the wireless community as a whole to come up with a new standard that addresses the weaknesses. Users started combining available technologies in order to reduce the risk of their wireless networks being penetrated to a level they were comfortable with. We all have information residing on our computers or transmitted over our networks that we want to keep out of the hands of others. Information which could be used to steal our identities or to steal our hard earned

money. This information includes, but is not limited to, our addresses, phone numbers, social security numbers, credit card numbers, bank account numbers, and usernames for websites, passwords for various websites and systems and pin numbers for anything from our bank cards to our home alarms.

In order to protect this valuable information, users started combining technologies. They would be sure to turn on WEP security in their wireless access points. But they would not stop their, they would employ authentication on their network through technologies such as 802.1x as implemented in EAP. They would create access lists of valid MAC addresses that could connect to their network. They would employed enhanced encryption by using virtual private networks deployed based on stronger encryption technology such as IPSec, SSL or SSH. However installing, configuring and getting all these technologies to work in concert in order to improve wireless security were not for the faint of heart however. You had to spend a lot of time getting each piece to work and only the most technically savvy users were able to protect themselves sufficiently. Given the large number of users, this meant only a small portion of the wireless community possessed the knowledge necessary to protect themselves while waiting for an improved standard to come along.

The Current Standard

There was a growing outcry from the user community for better security from wireless networks. Large sections of the network community made it known that they would stick with their wired networks and not deploy wireless networks until security of wireless networks was vastly improved.

Vendors have taken steps to respond to the outcry of the user community. Through firmware updates, they have provided new capabilities and changed default behavior of their hardware. No longer is it incumbent upon the user to turn the security features on in their routers. This is now the default setting. As stronger encryption becomes available, the vendors are making it available in their new products when bought and in their old products through updates. The user still has some responsibility here however. Even though security is turned on, it is using default values for the SSID, admin username and admin password. These values are widely known and readily available on the internet. As a result in order for the user to achieve a truly high assurance level of confidence in his networks security, he will have to be sure to change these default values when setting up his network.

The networking community has matured over the years and many members have gone to great pains to secure their networks from outside intruders. They have deployed intrusion prevention devices such as firewalls, hardened their operating systems, installed intrusion detection software, installed honey pots and taken many other well known steps to prevent unwanted access to their private networks.

Installing a wireless network router employing only WEP encryption technology would be like opening the backdoor, allowing an intruder to bypass all the other defenses they have erected to access of their network. Having established a need for something better, the wireless community responded. "The Wi-Fi Alliance, which tests and certifies products based on the 802.11 specification, recently approved a new security standard called Wi-Fi Protected Access (WPA), which addresses just about every WLAN vulnerability".[1]

Wi-Fi Protected Access

By moving away from WEP and introducing WPA, the wireless community has taken a giant step towards providing a secure wireless network which can only be accessed by authorized users. WPA includes user authentication and strong encryption. Lisa Phifer describes the benefits of WPA in this passage:

> WPA includes a new Temporal Key Integrity Protocol (TKIP) that uses key mixing and a longer initialization vector to overcome known problems in WEP that lead to key cracking. WPA also includes a real Message Integrity Check (MIC) called Michael that prevents wireless data from being modified in transit without detection. Finally, WPA manages keys to prevent static key reuse over long periods of time. In a home environment, WPA uses a shared secret passphrase to generate per-station encryption keys. In a business environment, WPA uses 802.1X port access control to distribute per-session keys to successfully authenticated stations, blocking WLAN access by all other stations. [9]

As can be seen by this passage, the wireless community has tried to address all known vulnerabilities in the original WEP standard. The also addressed the needs of both the home users with a small network and business users attempting to deploy a very large network in appropriate ways. To deal with the weak encryption provided by WEP, WPA employs temporal key integrity protocol (TKIP), 802.1X for dynamic key distribution and message integrity check (MIC). In order to address the lack of authentication available with WEP, WPA combines 802.1X with extensible authentication protocol (EAP). In other words, Wi-Fi Protected Access combines 802.1X, EAP, TKIP and MIC to close the well known openings inherent in the Wireless Encryption Protocol that was the previous security standard for wireless networks.

Products from vendors employing WPA technology are available on the shelves of stores today with additional products from other vendors on their way. In addition to this many vendors have made downloads available for updating their existing hardware to use WPA. If you are considering deploying a new wireless LAN today and you would like to protect the privacy of your network as well as

any information you transmit across the wireless LAN then at the very minimum you should be looking to purchase hardware which supports WPA.

As with WEP before it, the default configuration will already have the security features turned on by the vendor and you will simply have to change some default values so intruders knowing the readily available default values will not be able to use them to break into your network. WPA has also taken steps to make it easier to use the security settings such as allowing home users to share a secret pass phrase for generating their encryption keys. WPA works by generating per-packet keys and employing message integrity checking to ensure that the messages haven't been tampered while traveling across the wireless network. The best validation of the WPA has been provided by the fact that even though we are months beyond the release of the WPA specification to the user community, no one has identified a weakness in the scheme so far. This does not mean to imply that WPA provides perfect security, but simply that it is a well designed and thought out scheme for wireless security. This will help WPA in its goal of providing a high level of assurance to the community at large that their data will be safe when traveling over a properly configured wireless network which incorporates the WPA scheme for protection.

Now that we have implemented WPA in our wireless network, and taken the basic security steps necessary for any type of wireless network, we can update our analogy. Our network is now similar to house with doors locked and dead bolted and an alarm system with a code which is difficult to break. In other words, our wireless network now keeps out the honest but curious neighbor and common criminals who lack sophistication. At this point we should only be vulnerable to the criminals who possess sophisticated tools and a well developed knowledge of technology. And hopefully by being vigilante in how we deployed and configured our wireless network we have deterred these criminals and they will move on to attack someone with a more vulnerable set up.

WPA is a subset of 802.11i or WPA2 which is the future standard for wireless security.

A Glimpse of what's to come

The future of wireless security can be found in WPA2 (802.11i) which implements AES as its encryption technology. It is due to be released as a new security standard in early 2004. However, most of today's hardware is not powerful enough to provide both the strong protection provided by AES and still maintain the throughput required for our networks to be useful. This is supported by Jason Levitt who writes "The IEEE is expected to ratify 802.11i early next year, and it may appear in products as early as the third quarter of 2004." [12]

As a result of the processing demands imposed by WPA2 and AES, vendors will be releasing new, more powerful hardware in order to deploy this new standard. So don't be looking for too many downloads implanting WPA2 in the future, as most of the hardware currently available is inadequate to support it while maintaining their data throughput speed, which is their primary mission (security is secondary).

WPA2

Moving to WPA2 will provide a high level of assurance that your wireless network is secure. AES is a strong form of encryption sanctioned and used by the federal government. It comes in varying key strengths depending upon your needs. The most popular key sizes are 128 bit, 192 bit and 256 bit. For most home users this is more protection than they currently need, but should provide a feeling of security when connecting to and transferring data across their wireless LAN for the foreseeable future. As Leon Erlanger said "Both WPA and 802.11i show that the wireless LAN industry is finally getting serious about security." [1]

WPA2 will keep the user authentication and key management as used in WPA. The difference between WPA and WPA2 will be enhanced encryption. WPA2 will be replacing the current encryption algorithm with a robust algorithm that will need hardware assistance, known as Advanced Encryption Standard (AES).

The current plans for WPA2 are to support the WPA subset, allowing large organizations to slowly transition to the new standard. This will allow large organizations to purchase the new hardware in segments. They can start by deploying WPA2 capable access points. And then they can upgrade the clients (wireless access cards) in small groups or on a priority basis. Perhaps some users (accountants for example) deal with data considered more sensitive by the company. This would allow the company to purchase their updated hardware first, while perhaps deciding that WPA currently provides enough protection for users simply accessing email, allowing them to defer the purchases and spread the costs out over a longer period of time.

The networking community can have faith the abilities of WPA2 to provide protection for their computers and data. The encryption scheme is a strong one, based on sound mathematics and shown to be difficult to crack giving our current knowledge of mathematics and technology for at least the near future. Since the authentication and encryption schemes are well known, we can have more confidence in their strength. WPA2 has chosen the AES encryption scheme which requires hardware assistance to be able to implement the encryption/decryption while still providing acceptable throughput on the wireless network. This encryption scheme was thoroughly evaluated and selected by NIST as the government standard for encrypting and transmitting unclassified data. In terms of security we are always better off relying on sound mathematics and a publicly known encryption algorithm to protect our data than relying on keeping the algorithm secret. Because although we could base our secret

algorithm on sound mathematics, we couldn't ensure its robustness without exposing it to methods of attack we hadn't thought of. By providing the encryption algorithms to the public at large, we can have a higher degree of confidence that the algorithm is robust. The user community is made up of many talented people who think of new and different ways to attack problems all the time. Letting them try to attack your solution will either expose the weaknesses in it, or increase your confidence in it. WPA2 increases our confidence in the protection of our wireless data by being well known and thereby exposed to the unique attacks of talented individuals or groups.

The same precautionary steps taken earlier will still apply to WPA2. These steps include but are not limited to not broadcasting the SSID, limiting MAC addresses to your known wireless network cards, placing the access point in the center of the room, changing the SSID from the default value, changing the admin password from the default value and not setting the changed values to something easily guessed. Combining these protections with the enhanced authentication and encryption which will be available in WPA2 should provide peace of mind for even the most jaded segment of the user community.

This will provide us with the final update to our analogy. Once WPA2 is available and deployed in our wireless network, and assuming we have properly configured the settings and taken the proper physical precautions (location of the access point for example); then we can compare our wireless network to a house which has reinforced entrances, with strong difficult to pick locks and an alarm system which has a large difficult to guess code for access. In other words, the only people gaining access to our house at this time will be people who are known to have access and authorized to have access. This defense should be enough to deter most if not all of the criminals who want to access our property for whatever nefarious reason.

Conclusion

Wireless Networking got off to a bumpy start as far as security was concerned. Vendors did not give security a lot of thought and therefore delivered products that were insecure by default and had to be configured by the end user in order to provide even limited security. User authentication was not a consideration at the time and the encryption technology first delivered (WEP) was easily broken.

As the weaknesses of WEP and the default configurations of wireless routers were exposed, the wireless community responded to the problems. They encourage vendors to have security turned on by default, to provide user authentication and to strengthen the encryption technology. One consideration in the process was being able to strengthen security on the existing hardware deployed by users. The result of this is WPA which is just recently starting to penetrate the market. WPA provides user authentication and improved encryption on most existing hardware through a firmware upgrade. Vendors are

also providing resellers with hardware which includes the latest firmware and is configured to use the security features out of the box. The user is still required to change default settings such as user names and passwords and security set identifiers to improve protection, but at least the protection is now turned on by default.

However the wireless community is not stopping here as new techniques and improved hardware can make strong encryption algorithms weaker over time, therefore they are looking at incorporating stronger encryption techniques such as 256bit AES in the future. Their intent is that by being vigilant now and looking down the road they can keep ahead of the hackers and provide a very high assurance level to the wireless network community that their networks are safe and only accessed by authorized users.

To improve security further using WPA2 with AES will require new hardware. Some vendors are beginning to make this improved security option available to resellers. The future of wireless security looks poised to provide a high level of assurance that once properly configured (most of the configuration is provided by the default settings); your wireless network is secure and will only be used by authorized users.

Based on my look at wireless security I feel that great strides have been made by the wireless security community. We now have hardware available which provides strong authentication and encryption and addresses the known holes that previously existed. Research is continuing to work on improving wireless security by looking to identify any weaknesses in the current system and to fix the wireless network so that they can be deployed with a high degree of confidence. I look forward to hardware running WPA2 with 256bit AES that is reasonably priced. All connected systems come with risks, the future security implementation found in wireless networking appears to mitigate the risks enough to make this author consider replacing his current wired network with a wireless network protected by WPA2.

Given all this, I think the wireless networking community has taken a hard look at itself and provided consumers with a valuable interim solution while working on providing a comprehensive solution to the lack of confidence consumers have in current wireless networks. My only concern lies with the consumers themselves; there seems to be a rather blasé attitude towards computer security in general and wireless security in particular on their part. Consumers don't take the time to keep their virus definitions up to date, so I find it hard to believe they will take the time to install firmware upgrades on the wireless routers in order to improve security. Most of them don't change the default settings in their routers currently. Given this, I don't see deployed wireless security improving a great deal for years to come. I believe this will only happen when consumers purchase new hardware with strong security being its default setting and even then, many will not change the default usernames and passwords, thereby weakening the system provided

by the wireless community and undoing some of the positive steps the community has made.

References

1. Erlanger, Leon. “Real Security for Wireless LANs”. 5 Aug 2003. URL: http://www.pcmag.com/article2/0,4149,1194885,00.asp (Aug 2003)

2. Wi-Fi Alliance. “Wi-Fi Protected Access Overview”. URL: http://www.wi-fi.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf (Aug 2003)

3. “Security of the WEP algorithm”. URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (Aug 2003)

4. Phifer, Lisa. “Better Than WEP”. 1 Feb 2002. URL: http://www.ispplanet.com/fixed_wireless/technology/2002/better_than_wep.html (Aug 2003)

5. Loeb, Larry. “What's up with WEP?”. 1 Apr 2001. URL: http://www-106.ibm.com/developerworks/library/s-wep/ (Aug 2003)

6. Higgins, Tim. “WPA – Wireless security for the rest of us”. 1 Nov 2002 URL: http://www.smallnetbuilder.com/Sections-article35-page1.php (Aug 2003)

7. Higgins, Tim. “Need-To-Know: Wi-Fi Protected Access (WPA)”. 10 Jul 2003 URL: http://www.tomshardware.com/network/20030710/index.html (Aug 2003)

8. Phifer, Lisa. “Wireless Privacy: An Oxymoron?”. 26 Apr 2001. URL: http://www.isp-planet.com/technology/2001/wep.html (Aug 2003)

9. Phifer, Lisa. “Wireless Security”. 13 Dec 2002. URL: http://searchnetworking.techtarget.com/originalContent/0,289142,sid7_gci869140,00.html (Aug 2003)

10. Seltzer, Larry. “WPA To Whip Wireless Security into Shape”. 17 Jul 2003. URL: http://security.ziffdavis.com/print_article/0,4281,a=44907,00.asp (Aug 2003)

11. Internet Security Systems. “Wireless LAN Security 802.11b and Corporate Networks”. URL: http://documents.iss.net/whitepapers/wireless_LAN_security.pdf (Aug 2003)

12. Levitt, Jason. “Getting Serious about Wi-Fi Security Standards”. 3 Jul 2003. URL: http://www.iapplianceweb.com/story/OEG20030703S0014 (Aug 2003)