Wireless Security: WPA Vs WAPI, should we be worried?

Chris Rose

Technology Research Institute of Florida, Inc.

Abstract. *The IEEE 802.11 standard includes an optional encryption capability, the Wired Equivalent Privacy (WEP) however, WEP is vulnerable to attack and can easily be broken, therefore WEP was recently temporarily supplemented with Wi-Fi Protected Access (WPA) which offers improvements over WEP while a newer, more secure protocol 802.11i is developed. However, China has now introduced a new security protocol called WLAN Authentication and Privacy Infrastructure (WAPI) which is not a part of the IEEE 802.11 standard and is not interoperable with 802.11 which means that there will be two incompatible wireless security standards which will be inconvenient and more expensive for users. More importantly, because China is a large developing market, WAPI is an attempt by China to exert itself internationally as a major player in technological innovation by creating their own standard, even though this has the possibility to cause immense economic harm to established networking companies and disruption in the worldwide technological infrastructure.*

Introduction

Wireless networking has brought convenience to both the home and office since it is now possible to abandon the wires which formally connected all the computers in a network together. The problem with wireless is that unlike wired networks where data travels over physical cables or fiber, the wireless LAN broadcasts signals in the air and these can be intercepted by anyone within range. Although most wireless LANs implement an encryption scheme, the authentication protocols are also broadcast through the air and these can be intercepted by an eavesdropper who can then generate a key and decrypt the data.

WEP – a Brief History

The IEEE 802.11 standard includes an optional encryption capability called Wired Equivalent Policy (WEP), which uses the RSA RC4 security algorithm in the media access controller (MAC). With WEP all the passwords are stored in both the access points and on each computer on the network with the intention that WEP will

Rose C. (2004).
Wireless Security: WPA Vs WAPI, should we be worried?.
In *Proceedings of the 3rd International Workshop on Wireless Information Systems*, pages 18-23
DOI: 10.5220/0002682800180023

encrypt all the transmissions between the access point and the devices on the network. This encryption does not implement a high level of security in a public network, since it would also have to publish the password [8].

WEP was designed with the following factors in mind:

- Reasonably strong - It must meet customers' needs.
- Self-synchronizing - Stations quite frequently go in and out of coverage.
- Computationally efficient - The WEP algorithm may be implemented in hardware or software. If it is efficient, it allows low-MIPS devices to still implement it in software.
- Exportable - It can be exported outside the US and imported to other countries.
- Optional - It is an option not required in an 802.11-compliant system [12]

WEP specifies the use of 40 bit keys and this type of key was chosen because at the time the protocol was drafted, the United States Government had restrictions on the export of technology containing cryptography. However, this key length is short enough to make brute force attacks easily accomplished with just about any amount of computing power available today. However, many equipment manufacturers extend this protocol and offer a stronger encryption in the form of a 128-bit key, which is really a 104-bit key with a 24-bit initialization vector (IV). By using this extension, brute force attacks are nearly impossible with today's computing platforms but there are other methods that do not require an attack on the key, so even the 128-bit key is not totally secure.

Various vulnerabilities have been demonstrated with WEP and among these are those documented by Borisov, Goldberg and Wagner (2001) [2] who demonstrated four types of attacks that are easily perpetrated on wireless networks by anyone using readily-available, off-the-shelf equipment. These are:

1. Passive attacks to decrypt traffic based on statistical analysis.
2. Active attack to inject new traffic from unauthorized mobile stations, based on known plaintext.
3. Active attacks to decrypt traffic, based on tricking the access point.
4. Dictionary-building attack that, after analysis of about a day's worth of traffic, allows real-time automated decryption of all traffic.

WPA – the Temporary Solution

Because WEP has been found to be vulnerable to attacks, various alternatives have been investigated. The Wireless Ethernet Compatibility Alliance (WECA) is the industry group that verifies and certifies 802.11x wireless products for interoperability. On January 21, 2002, WECA (also called the Wi-Fi Alliance) completed a draft of IEEE's 802.11i spec to improve security on 802.11 wireless networks and this is now being circulated within the engineering community for editing and eventual approval. This draft is for a security algorithm called Temporal Key Integrity Protocol (TKIP) which was developed with the help of some of the same encryption experts that exposed the vulnerabilities in WEP. Although TKIP, like WEP, is based on RC4 encryption it is implemented in a different way that addresses some those vulnerabilities, including the ability to generate a new set of encryption

keys for every 10,000 packets. Most current Wi-Fi certified products should be upgradeable to TKIP and those that cannot be upgraded will still interoperate with products that use TKIP but will only use WEP for security [1].

However, not all researchers are satisfied that TKIP will be able to do what it is designed to do. Some researchers believe the real problem is the fundamental way in which Wi-Fi works. Although rapid rekeying of WEP keys, which will be implemented in TKIP, will make it more difficult to crack, the complete design is not good security. If you are relying on a confidentiality mechanism, in general that is considered bad design and TKIP does not eliminate the fundamental flaw in Wi-Fi security. "If anybody breaks TKIP, they not only break the confidentiality but they also break the access control and authentication so one break breaks everything. That is not good design. Each security mechanism should stand on its own" [9].

However, TKIP is just considered an interim solution for WEP that mandates that each client uses different keys and frequently changes them before a hacker has time to decipher them. TKIP uses a 128 bit key along with the user's MAC address plus an initialization vector. In May 2002, the U.S. Secretary of Commerce chose the Advanced Encryption Standard (AES) which is up to 256 bits and is even stronger than DES, as an authorized government standard and it will eventually supersede the Data Encryption Standard (DES) in new deployments. However, companies with deployed wireless LANs can upgrade their networks to TKIP security using firmware. AES requires hardware acceleration using a co processor to off load the encryption and decryption or it would slow the throughput down to an unacceptable level. It also requires new Wi-Fi cards in the client devices and new access points. AES was available in the first quarter of 2003 [9].

The Wi-Fi Alliance has certified Wi-Fi Protected Access (WPA) and although it is not an official IEEE standard, it has been adopted by the Wi-Fi Alliance as a temporary measure as an enhancement to the security of wireless networks until work on 802.11i has been completed [6]. WPA is used with TKIP and the Michael message integrity check (MIC) algorithm, to provide enhanced security for wireless networks

The Michael security algorithm calculates an 8-byte Message Integrity Code (MIC) and this uses a calculation features which is available on existing wireless devices. The calculated MIC is placed between the data of the IEEE 802.11 frame and the 4-byte ICV. The MIC field is encrypted together with the frame data and the 4-byte Integrity Check Value (ICV). In addition, Michael provides protection against replay attacks and it does this by including a new frame counter in the IEEE 802.11 frame.

WAPI

The 802.11i security standard went out to be voted on for confirmation in late 2003 (to date no results are available) but in a surprising twist, the Chinese government has announced their own specification. The Standardization Administration of China (SAC) announced in May 2003, that China would adopt a WLAN standard, called GB15629.11-2003. The WLAN equipment that is sold in China is required to comply with this standard from Dec. 1, 2003 but a transition

period has been granted and this extends the compliance deadline for a few WLAN products until June 1, 2004 [6].

The recently announced Chinese WLAN standard is very similar in many ways to the IEEE's 802.11 wireless networking standard but the one important difference is that it uses a security protocol, called WLAN Authentication and Privacy Infrastructure (WAPI). WAPI is not part of the 802.11 standard, since the IEEE standard relies on Wired Equivalent Privacy (WEP). However, if there are two different WLAN standards in existence, one for China and one for the rest of the world, this could cause the market for wireless networking equipment to splinter in two [6].

WAPI uses a block cipher for encryption and an authentication mechanism that appears to be similar to the IEEE 802.1x standard, which is part of the upcoming IEEE 802.11i security standard. Diagrams shown during technical discussions with Chinese officials indicated something like a RADIUS (Remote Authentication Dial-In User Service) server being used for authentication and in addition, they seemed to show a central RADIUS system for authenticating all users on all WLANs in China [6]. This is possibly a method of monitoring all wireless devices being used in China.

In addition, this new Chinese specification will possibly cost more and be harder to integrate into portable devices like PDAs and phones since it will probably require more memory. This might also affect the entire notebook market since it will have an effect on other products that utilize wireless networking. To make matters worse, if a foreign vendor wishes to produce a product that complies with this new Chinese standard then they have to sign coproduction agreements with a limited number of specifically designated Chinese companies, which China justifies by citing national security concerns. However, the foreign company would have no control over what goes inside these security products, which obviously raises liability questions, and of course the Chinese company might simply delay production for the foreign company giving alternative Chinese manufacturers an unfair advantage. Even more worrying is that these Chinese firms might demand full disclosure of the foreign technology, claiming it is impossible to implement WAPI without this information [6].

Since China is the most important developing economy in the world and it accounts for a large portion of manufactured goods, including high-tech products, China will in the next few years, become a major power in engineering and technology. One method of establishing a country for a position of leadership in technology is to set national standards that are incompatible with what the rest of the world is doing. What in effect this does is that it forces everyone else to deal with technologies that are otherwise unnecessary and this can be used to protect domestic industries [7].

What is happening is that the world’s most populous nation, with the world’s fastest growing economy, which will shortly be the second most important market for computer products (after the USA) is flexing their muscles. This is not the first time that China has done this as they have their own version of Linux called RedFlag, their own CPU architecture called Dragon and just recently implemented their own proprietary DVD standard. Perhaps this is also related to the Chinese government’s effort to develop products that are not subject to the payment of patent royalties which

they are now obligated to pay ever since they joined the World Trade Organization. Skeptics might consider WAPI to be just another effort at this.

Standards and Network Externalities

The concept of a network externality emerges from the fact that some goods and services are more valuable when more people consume or utilize that good or service and yet these goods and services have little or no value if they are used without a network [4]. Examples of network externalities include telephones and fax machines as people who own these products would form a network so as to be able to exchange information and provide a way for people to communicate with each other. The more people who have telephones the more valuable this network becomes and the same applies to wireless network equipment. In markets where network externalities are powerful and people are able to choose from different standards, the advantages of conforming to a popular platform must be weighed against the advantages of horizontally differentiating output since conforming to a common standard exploits the added value associated with network externalities [3].

If a specific technology penetrates a significant portion of the market for any product, it becomes extremely difficult to dislodge simply because people do not wish to switch to a new piece of hardware or software, even if the new product is proven to be superior. This is because they will lose both the time they invested in the old product and the ability to share data with others who would also have the old product [11]. This is exactly what has happened with the 802.11 standard, in fact, what has occurred is that the wireless network 802.11 standard has effectively caused a lock-in. “A lock-in occurs when the self reinforcing effects increase demand for a specific product or service and make it difficult for innovative alternatives to be considered” [5]. Since a de facto lock-in has occurred with 802.11 throughout the rest of the world, it will be extremely difficult for China’s WAPI to succeed outside of China, but the problem will exist for manufacturers who wish to sell goods to China or for visitors to China who wish to use their 802.11 equipment.

Conclusion

Although WAPI has been portrayed as the Chinese solution to the problem of wireless security it appears to have many of the same problems as WEP. Many believe that WAPI will be insecure and cause problems for manufacturers who will now have to conform to two standards, one for China and another for the rest of the world [10].

It is also left to be seen if the rest of the world will accept this Chinese wireless standard. For an encryption standard to be thought of as trustworthy, it would first have to be written by a well-respected member of the cryptography community and be also subjected to many years of peer review, and only if it is able to survive without any major weakness being discovered will it be accepted in the encryption

community. It is very doubtful that China would open up their standard for peer review by the rest of the world.

In addition, since the 802.11 standard has enjoyed worldwide acceptance, network externalities are very strong which has caused a lock-in, whereby people are going to be resistant to move to another wireless standard. Therefore, while WAPI will enjoy government mandated success in China and cause severe disruptions among foreign wireless technology companies that wish to sell their products in the Chinese market, it will not penetrate the market outside of China. Unfortunately, it will also cause immense inconvenience for foreign visitors in China.

References

1. Arar, Y.: Beefing up 802.11b Security PCWorld (2002, February 4)
2. Borisov, N. Goldberg, I., Wagner, D.: Intercepting Mobile Communications: The Insecurity of 802.11. Proceedings of the 7th International Conference on Mobile Computing and Networking, Rome, Italy (July, 2001)
3. Economides, N., Flyer, F.: Compatibility and Market Structure for Network Goods. New York University. (November, 1997)
4. Katz, M., Shapiro, C.: Network Externalities, Competition and Compatibility. American Economic Review (June 1985)
5. Krechmer, K.: The Fundamental Nature of Standards: Economics Perspective Communications Standards Review (2000)
6. Lemon, S., Lawson, S.: Clouds hang low over Chinese WLAN standard IDG News Service. (December 19, 2003). Retrieved from the World Wide Web on 1/14/04 from http://wireless.itworld.com/4276/031219chinawlan/page_1.html
7. Mathias, C.: Chinese food for thought. EETimes. (January 5, 2004) Retrieved from the World Wide Web on 1/14/04 from http://www.eetimes.com/comm/c/rd/OEG20040105S0043
8. Oraskari, J.: Bluetooth versus WLAN IEEE 802.11x. Department of Computer Science and Engineering, Helsinki University of Technology (2001)
9. Schwartz, E.: Researchers crack new wireless security spec. InfoWorld (February 14, 2002)
10. TIA: China Promotes New Wireless Encryption Standard. Pulse Online. (December 2003) Retrieved from the World Wide Web on 1/14/04 from http://pulse.tiaonline.org/article.cfm?ID=1911
11. Varian, H.: The Information Economy: How much will two bits be worth in the digital marketplace? Scientific American (September 1995)
12. Weatherspoon, S.: Overview of IEEE 802.11b Security. Intel Technology Journal (2000, Q2)