Wireless Network Security : Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) Security Protocols.

Halil Ibrahim BULBUL
Gazi University
06830 Gölbaşı, Ankara
+90 312 4851124
bhalil@gazi.edu.tr

Ihsan BATMAZ
Gazi University
06500 Beşevler, Ankara
+90 312 202 8645
ibatmaz@gazi.edu.tr

Mesut OZEL
Gazi University
06830 Gölbaşı, Ankara
+90 312 4851124
mesutozel@yahoo.com

ABSTRACT
Wireless Local Area Networks (WLANs) are gaining popularity as they are fast, cost effective, flexible and easy to use. They are, however, faced with some serious security challenges and the choice of security protocol is a critical issue for IT administrators.

The goal of this paper is to make the non-specialist reader aware of the disadvantages and threats of the wireless security protocols. WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) security protocols are examined in this respect. Then they are compared via the common features in order to give some insight to those who work with WLANs. We hope this paper give boost to the IT security staff and clarify the common questions of the non-specialist reader.

This paper is a compilation of the wireless security weaknesses and counter measures that are put forward until recently. We believe that a thorough understanding of this paper makes the non-specialist reader have a complete review of wireless security and vulnerabilities associated with it.

Key words : Wireless Security, WEP, WPA, WPA2, RSN.

1. INTRODUCTION

The major difference between wired and wireless networks is the way that how they transmit data. As for the security risks, the main difference between wired and wireless networks is how to access to the transmitted data. In wired networks this is only possible by tapping the media that is used for the network communication. In wireless networks the media used for communication is air. The transmitted data via the radio frequency can be accessed by equipment that is readily available in the market for a cheap price.

From the initial development stages of wireless technology and its security needs, experts knew that security would be the major issue. Wireless Networks are inherently less secure than traditional wired networks, since they broadcast information into the air and anyone with in the range of and with the right equipment can easily intercept those transmissions. It is for sure that matching all security needs of a wireless network is not an easy task. There are a number of security issues that make securing a WLAN difficult [1].

The latest studies [2,3] show the reasons for what their motives are and why organizations implement wireless networks. In spite of the motives for implementation of wireless networks, the most important drawback with wireless technology according to the participants is security. Although WLAN security seems very challenging, most of the risks could be addressed by reasonable security precautions. The general challenges to be addressed are discussed in [4, 5, 6, 7, 8].

2. WLAN SECURITY MECHANISMS AND PROTOCOLS

2.1. WLAN Security in General

Since WEP is the initial and so-called WLAN security mechanism of all aforementioned protocols, it is aimed to cover it in a broader perspective than WPA/WPA2 and RSN. Several serious weaknesses were identified by cryptanalysts in WEP, and WEP was superseded by Wi-Fi Protected Access (WPA) in 2003, and then by the full IEEE 802.11i standard RSN (also known as WPA2) in 2004 ratified.

2.2. Wired Equivalent Privacy (WEP) Mechanism

WEP was intended to give wireless users a security scheme that is equivalent to being on a wired network. The main intention of the WEP was not to provide a level of security superior to or higher than that of a wired LAN, but equivalent to it. So the name of the protocol, "Wireless Equivalent Privacy - WEP" signifies the actual intention of the developers [9].

However, the practice has shown that the level of security offered by WEP hardly equivalent to the level of security provided by wired LANs. Despite the weaknesses in the protocol, some may argue that WEP provides a level of security that can deter casual snooping.

2.2.1. How WEP works

When WEP is active each 802.11 packet is encrypted separately with an RC4 cipher stream generated by a 64-bit RC4 key. This key is composed of a 24-bit Initialization Vector (IV) and a 40-bit WEP key. The encrypted packet is generated with a bitwise exclusive OR (XOR) of the original packet and the RC4 stream. The IV is chosen by the sender and can be changed periodically so every packet won't be encrypted with the same cipher stream. The IV is sent in clear with each packet. An additional 4-byte Integrity Check Value (ICV) is computed on the original packet and appended. The ICV is also encrypted with the RC4 cipher stream [10]. How WEP encryption works is depicted in Figure-1.

e-Forensics 2008, January 21-23, 2008, Adelaide, Australia.

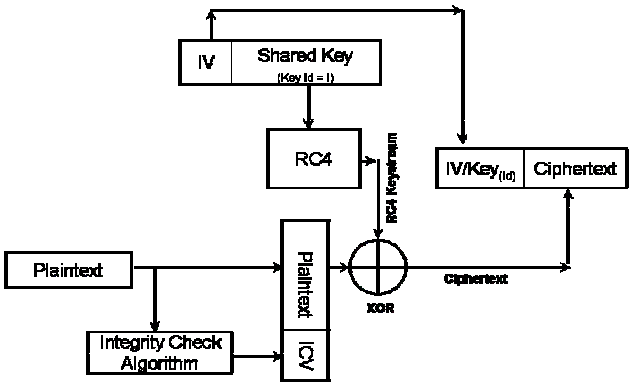

Figure -1 WEP Encryption

2.2.2. Vulnerabilities and flaws of WEP

As it has been noted earlier, WEP uses the RC4 stream cipher with a 24- bit Initialization Vector for encryption. The design of WEP makes the system vulnerable in many areas, and one of the weakest parts of WEP is the 24-bit Initialization Vector, which may result in key stream reuse. Key stream reuse in turn permits successful cryptanalysis attacks against the cipher text. So WEP has been accepted as a fail to accomplish security goals and contains major security flaws [11].

Another vulnerable aspect of the WEP is the use of CRC-32 mechanism used for the integrity check. CRC (Cyclic Redundancy Code) is defined as a class of "checksum" algorithms that operate by treating any message as a large binary number and then dividing it in binary without overflow by a fixed constant. The remainder is called the "checksum". And it is known that CRC is not cryptographically strong and not intended to be used in place of message digest or hash functions. Due to the nature of CRC, it fails to provide the required integrity protection. One must keep in mind that the usage of CRC-32 was intended as a security measure in WEP, which isn't true. CRC-32, as being fast, yet is no better solution than a slower and secure solution.

Weaknesses in the Key Scheduling Algorithm of RC4 are put forward in [12]. A passive cipher-text-only attack against the key scheduling algorithm of RC4 as used in WEP has been described. By identifying a large number of weak keys, in which knowledge of a small number of key bits suffices to determine many state and output bits with non-negligible probability. Additionally the first byte generated by the RC4 leaks information about individual key bytes. So by analyzing enough WEP-encrypted packets it could be possible to reconstruct the secret key in WEP.

The authentication flaws in the IEEE 802.11 are put forward by [13]. Based on the knowledge obtained by [11] it was demonstrated that a simple successful eavesdropping attack against IEEE 802.11 authentication was possible even with WEP on.

The recovery of the 128 bit secret key used in a network, using a passive attack technique was mentioned to be successful as in [12]. Since standard WEP uses RC4 and IVs improperly, applied attack exploited this design failure. So it was concluded that 802.11 WEP is totally insecure and that it is the poor implementation of reasonable secure technologies (such as RC4) that is responsible for WEP weaknesses [14].

In response to the aforementioned studies [11, 12, 13, 14, 15, 16] about the insecurity of WEP, WECA has published an official statement, clarifying its understanding of the situation. The bottom line of this statement was that a poor security is better than no security. And WEP was not intended to be a solution for all security needs. The statement notes that the biggest security threat is the failure to use available protection methods, including WEP [17, 18].

2.2.3. The weaknesses of WEP

-Use of Master keys directly: From the cryptographic point of view, using master keys directly is not at all recommended. Master keys should only be used to generate other temporary keys. WEP is seriously flawed in this respect.

-Small key size: The key size of the key for WEP is 40 bits, which has been cited as one of the major weaknesses of WEP. In 1997, 40-bit keys were considered to be reasonable for some applications. Since the goal was to protect against casual eavesdropping, it seemed sufficient at the time. The 802.11 standard does not specify any WEP key sizes other than 40 bits. But most vendors apply the key size to 104 or 232 bits. But in either case the RC4 encryption key includes a 24-bit IV. It is for sure, 104 and 232-bit keys are more resistant to brute-force attacks than 40-bit keys but did not resolve the problem.

-Lack of key management: Key management is not specified in the WEP standard. Since without interoperable key management, keys will tend to be long-lived and of poor quality. Most wireless networks that use WEP have one single WEP key shared between every node on the network. Access points and client stations must be programmed with the same WEP key. Since the change of keys task is tedious and difficult, they are rarely changed by the system administrators.

-Use of RC4: WEP's RC4 implementation has been considered to have weak keys, meaning that there is more correlation between the key and the output than there should be. Determination of which packets were encrypted with weak keys is an easy job. Since the first three bytes of the key are taken from the IV that is sent unencrypted in each packet, this weakness can be exploited easily by a passive attack.

Out of the 16 million IV values available, about 9,000 are interesting. They indicate the presence of weak keys. The attacker captures "interesting packets" filtering for IVs that suggest weak keys, then analyzes them and only has to try a small number of keys to gain access to the network. Because all original IP packets start with a known value, it's easy to know when he/she has the right key. To determine a 104-bit WEP key, he/she has to capture between 2,000 and 4,000 interesting packets. On a fairly busy network the capture of the interesting 5,000 packets might not pose any difficulty and can be achieved in a short period of time [15, 17]. Many vendors are now implementing new algorithms that simply do not choose weak IVs since the best defense against this type of attack is not to use weak IV values. But, if just one station, on the network uses a weak key, then the attack can succeed.

-Reused and small sized IV's: Regardless of the key size, 24-bit long of WEP's IV can only provide 16,777,216 different RC4 cipher streams for a given WEP key. On a moderately busy network this number can be achieved in a few hours and reuse of the same IV then becomes unavoidable. In WEP the RC4 cipher stream is XOR'ed with the original packet and the IV is sent in the clear format with each packet. If the RC4 cipher stream for a given IV is found, an attacker can decrypt subsequent packets that were encrypted with the same IV or can forge packets.

Since there are maximum 16,777,216 IV values, how the IV is chosen makes a big difference. Unfortunately, WEP doesn't specify how to choose or how often to change IVs. Some implementations start the IV at zero and increase it incrementally for each packet, rolling over back to zero after 16 million packets have been sent. And some other implementations choose IVs randomly which sounds like a good idea. But it really isn't. With a randomly chosen IV, there is a 50% chance of reuse after less than 5,000 packets as put forward in [15].

-Weakness of ICV algorithm: WEP ICV is based on CRC-32, an algorithm for detecting noise and common errors in transmission. CRC-32 is an excellent checksum for integrity and detecting errors, but it is not a good choice of cryptographic hash.

The CRC-32 ICV is a linear function of the message meaning that an attacker can modify an encrypted message and easily fix the ICV so the message appears authentic. Having able to modify encrypted packets provides for a nearly limitless number of very simple attacks. An attacker can easily make the victim's wireless access point decrypt packets for him. This is simply done by capturing an encrypted packet stream, modifying the destination address of each packet to be the attacker's wired IP address, fixing up the CRC-32, and retransmitting the packets over the air to the access point. The access point will happily decrypt the packets and forward them to the attacker. IV and ICV based attacks are independent of the key size; even with huge key sizes the attack takes the same amount of effort.

-Easy forging of authentication messages: 802.11 standards declare two types of authentication; Open System and Shared Key authentication. The theoretical idea was that an authentication would be better than no authentication. But in reality the opposite is emerged to be true. Turning on authentication with WEP, actually reduce the total security of the network and make it easier to guess WEP key for the intruders and attackers.

Shared Key authentication involves demonstrating the knowledge of the shared WEP key by encrypting a challenge. The problem here is, any monitoring attacker can observe the challenge and the encrypted response. From those, then can determine the RC4 stream used to encrypt the response, and use that stream to encrypt any challenge he/she would receive in the future. So by monitoring a successful authentication, the attacker can later forge an authentication. The only advantage of Shared Key authentication is that it reduces the ability of an attacker to create a denial-of-service attack by sending garbage packets (encrypted with the wrong WEP key) into the network [14]. To handle the task of proper authenticating wireless users turn off Shared Key authentication and depend on other authentication protocols, such as 802.1x [18].

As it has been put forward above, WEP is found to be far from an ideal security solution but it could be still used. Having a security mechanism as a deterrence shield is better than having none. Any determined attacker may be able to discover WEP keys, given time and enough weak IVs, but that might not be the reason to leave all of the doors to the system open.

2.3. Wi-Fi Protected Access (WPA) Protocol

The first wireless security solution for 802.11-based networks, Wired Equivalent Privacy (WEP), received a great deal of coverage due to various technical failures in the protocol. So, the standards bodies and industry organizations have been spending a great deal of time and money on developing and deploying next-generation solutions that address growing wireless network security problems. Taking into consideration of the vulnerabilities and flaws in WEP, the Wi-Fi (Wireless Fidelity) Alliance, has created the Wi-Fi Protected Access (WPA) standard which is a subset of the 802.11i draft.

2.3.1. Enhancements Over WEP

WPA was designed to improve upon the security feature deficits of WEP. The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA technology mainly includes three improvements over WEP:

-Improved data encryption through the Temporal Key Integrity Protocol (TKIP). This scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. TKIP, is a Temporal Key Hash Function and it is an alternative to WEP that fixes all the security problems and does not require new hardware. Like WEP, TKIP uses the RC4 stream cipher as the encryption and decryption processes and all involved parties must share the same secret key. This secret key must be 128 bits and is called the "Temporal Key" (TK). TKIP also uses an Initialization Vector (IV) of 48-bit and uses it as a counter. Even if the TK is shared, all involved parties generate a different RC4 key stream. Since the communication participants perform a 2-phase generation of a unique "Per-Packet Key" (PPK) that is used as the key for the RC4 key stream.

-User authentication, which is missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network. For detailed information about EAP please refer to [18].

-Integrity, a new mechanism, Message Integrity Code (MIC) for TKIP is computed by a new algorithm namely "Michael" [20]. Message Integrity Code (MIC) is computed to detect errors in the data contents, either due to transfer errors or due to purposeful alterations. The new MIC for TKIP is computed by a new algorithm called "Michael" [21]. It is a 64-bit MIC that is added to the Data and the ICV. The ICV is CRC of Data and MIC.

2.3.2. What is new in WPA in comparison to WEP?

-Master keys are used directly in WEP: Master Keys are never used directly in WPA. A hierarchy of keys is used, all derived from the master key. Cryptographically this is much more secure.

-Key Management and updating is poorly provided for in WEP: Secure key management is a built-in feature in WPA, so key management isn't an issue with WPA as compared to WEP.

-IV values can be reused/IV length is too short: In order to eliminate the rollover of counter and reuse of the keys, the length of the IV has been increased from 24 bits to 48 bits. Additionally, IVs are used as sequence counters for the TSC (TKIP Sequence Counter), protecting against replaying of data, which was a major vulnerability in WEP.

-Weak IV values are susceptible to attack: WPA avoids using known weak IV values. A different secret key is used for each packet, and the way the key is scrambled with the secret key is more complex.

-Message integrity checking is ineffective: WEP message integrity protocol CRC-32 was proved to be ineffective so WPA uses a Message Integrity Check (MIC) mechanism called, 'Michael'. In theory there is a one in a million chance of guessing the correct MIC. In practice any changed frames would first need to pass the TSC and have to have the correct packet encryption key even to reach the point where 'Michael' comes into operation.

2.3.3. One Alleged Drawback Associated With WPA

The 802.11i standard points out that keys generated from short passwords are subject to dictionary attack and a key that is generated from a pass phrase of less than 20 characters is unlikely to deter attacks. But using a pass phrase more 20 characters long is considerably longer than most people will be willing to use. Otherwise an offline attack would be easier to execute than the WEP attacks [22].

2.4. Robust Security Networks – RSNs

802.11i that has been emerged in 2004 uses the concept of a Robust Security Network (RSN), where wireless devices need to support additional capabilities. This new standard and architecture utilizes the IEEE 802.1X standard for access control and Advanced Encryption Standard (AES) for encryption. It uses a pair-wise key exchange (four way handshake) protocol utilizing 802.1X for mutual authentication and key management process [23].

802.11i allows for various network implementations and can use TKIP, but by default RSN uses AES (Advanced Encryption Standard) and CCMP (Counter Mode CBC MAC Protocol) and it is this which provides for a stronger, scalable solution [24].

2.4.1. How RSN Works

RSN uses dynamic negotiation of authentication and encryption algorithms between access points and mobile devices. The authentication schemes proposed in the draft standard are based on 802.1X and Extensible Authentication Protocol (EAP). The encryption algorithm is Advanced Encryption Standard (AES).

Dynamic negotiation of authentication and encryption algorithms lets RSN evolve with the state of the art in security. Using dynamic negotiation, 802.1X, EAP and AES, RSN is significantly stronger than WEP and WPA. However, RSN would run very poorly on legacy devices. Unfortunately only the latest devices have the capability required to accelerate the algorithms in clients and access points, providing the performance expected of today's WLAN products.

2.4.2. Assessment of RSN

WPA had improved security of legacy devices to a minimally acceptable level with one exception mentioned earlier (pass phrases not less than 20 characters), but RSN is the future of over-the-air security for 802.11 as put forward in [25].

3. COMPARISON OF WEP MECHANISM, WPA AND RSN SECURITY PROTOCOLS

3.1. Discussion of Findings in Table-1

WEP has been regarded as a failure in wireless security, as it has been accepted by the IEEE that WEP was not aimed to provide full security. The original WEP security standard, using RC4 cipher is widely considered to be vulnerable and broken due to the insecure IV usage. It uses 40 bits of encryption key RC4 cipher by default (with vendor specific longer key support exceptions), concatenates key with IV values per packet sent over the air, with no key management mechanism embedded, having no automatic or periodic key change attribute associated with it, causing re-use and easy to capture small sized IVs that leads to key deciphering to the third parties. The data integrity check mechanism of WEP is not cipher protected and uses CRC-32, ICV providing no header integrity control mechanism and lack of replay attack prevention mechanism.

WPA, an interim solution to the WEP vulnerability, uses a subset of 802.11i features and had been generally believed as a major security improvement in wireless environment. In the light of critics done towards WEP, WPA has numerous enhancements over WEP. Namely, RC4 – TKIP encryption cipher mechanism, 128 bits of key size, mixed type of encryption key per packet usage, 802.1x dynamic key management mechanism, 48 bits of IV size, 802.1x – EAP usage for authentication, providing data integrity and header integrity, ciphering aspect via MIC that is inserted into TKIP and IV sequence mechanism to prevent replay attacks and support for existing wireless infrastructures [26, 27].

Table-1.Comparison of WEP Mechanism, WPA and RSN Security Protocols.

Features of Mechanism	WEP	WPA	RSN
Encryption Cipher Mechanism	RC4 (Vulnerable - IV Usage)	RC4 / TKIP	AES / CCMP CCMP / TKIP
Encryption Key Size	40 bits *	128 bits	128 bits
Encryption Key Per Packet	Concatenated	Mixed	No need
Encryption Key Management	None	802.1x	802.1x
Encryption Key Change	None	For Each Packet	No need
IV Size	24 bits	48 bits	48 bits
Authentication	Weak	802.1x - EAP	802.1x - EAP
Data Integrity	CRC 32 - ICV	MIC (Michael)	CCM
Header Integrity	None	MIC (Michael)	CCM
Replay Attack Prevention	None	IV Sequence	IV Sequence
(*) Some vendors apply 104 and 232 bits key, where the 802.11 requires a 40 bits of encryption key.			

RSN seems to be the strongest security protocol for wireless networks as far as all previously declared vulnerabilities and drawbacks pertaining to WEP and WPA concerned. After the 802.11i standard ratified RSN is accepted as the final solution to wireless security, expected to provide the robust security required for wireless environments. RSN provides all the advantages of WPA in addition to stronger encryption through the implementation of AES, roaming support and CCM mechanism for data and header integrity.

WPA supports existing wireless infrastructures. WPA deployments over current WEP installations provide cost effective and hassle free shifts where vendors can transit to the WPA standard through a software or firmware upgrade. For RSN this is not the case. It requires extra hardware upgrade in order to implement AES.

4. CONCLUSION

Wireless networks can be a significant tool in increasing business productivity. As more implementations of wireless networks emerge due to user demand, the IT staff responsible for the system security have to understand the security threats that wireless technology poses. People who are after this technology need to plan and take proper security measures before and after implementing wireless networks in their environment to protect data.

However, as discussed in this paper, wireless networks bring with them a totally new set of security risks which must be evaluated and countered proactively. Often IT staff overlook the importance of wireless security. Therefore, they need to understand the strengths and weaknesses of wireless technology, so they can take the appropriate steps to address those security issues.

With current technology one may insist that there is no reason not to trust a well setup wireless network but the cost of possible vulnerability exploitation is worth considering proactively. WLANs that are not managed properly might cause very serious risks to companies. So before installing any such networks, all risks must be identified, evaluated, and based on the results, the necessary counter measures must be installed to secure the network.

Although no security system can ever be considered totally unbreakable, 802.11i RSN security seems to be a dependable one. It suffers none of the problems of older mechanisms and protocols namely WEP and WPA. So 802.11i RSN is a wireless security protocol that any body can rely on until its vulnerabilities are brought out.

For the time being in terms of cost versus security options, if full security preferred then RSN must be employed, if minimum cost preferred WEP must be employed, other wise usage of WPA is recommended.

5. REFERENCES

[1] Manley, M.E.; McEntee, C.A.; Molet, A.M.; Park, J.S.; **Wireless Security Policy Development for Sensitive Organizations,** Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005. Proceedings from the Sixth Annual IEEE, 15-17 June 2005 Page(s):150-157

[2] Boland, H.; Mousavi, H., **Security issues of the IEEE 802.11b wireless LAN,** Electrical and Computer Engineering, 2004. Canadian Conference on, Volume 1, 2004 Page(s):333-336 Vol.1.

[3] **2003 Wireless LAN Benefits Study**, Conducted by NOP World Technology on Behalf of Cisco Systems November, 2003. http://newsroom.cisco.com/dlls/2003_NOP_WLAN_Benefits_Study.pdf#search=%222003%20Wireless%20LAN%20Benefits%20Study%20%22

[4] Mishra, A., Petroni, N.L., and Arbaugh, W.A., Fraser, T., **Security Issues in IEEE 802.11 Wireless Local-Area Networks: A Survey,** Wireless Communications and Mobile Computing Journal, Vol. 4, No. 8, Page(s):821-833, 2004.

[5] Karnik, A.; Passerini, K.;**Wireless Network Security - A Discussion From a Business Perspective,** Wireless Telecommunications Symposium, 2005, 6-7 April 2005 Page(s):261 - 267

[6] Gast M., **Seven Security Problems of 802.11 Wireless.** http://www.oreillynet.com/lpt/a/2404

[7] Welch D. and Lathrop S., **Wireless Security Threat Taxonomy,** Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society, NY 18-20 June 2003 Page(s):76 – 83.

[8] Loeb L., **Roaming charges: Threat taxonomy**, **The real scoop on wireless network security at West Point.** http://www-128.ibm.com/developerworks/wireless/library/wi-roam15.html

[9] ANSI/IEEE Std 802.11, 1999 Edition (R2003), **Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,** Section 8, Authentication and privacy, Sub section 8.2.1, Page:61,

[10] Wikipedia, The Free Encyclopedia. http://en.wikipedia.org/wiki/RC4

[11] Borisov. N., Goldberg, I., Wagner, D., **Intercepting Mobile Communications :The Insecurity of 802.11.** http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf

[12] Fluhrer, S., Mantin, I., Shamir, A., **Weaknesses in the Key Scheduling Algorithm of RC4.** http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf

[13] A. Arbaugh,W., Shankar N., Justin Wan,Y.C., **Your 802.11 Wireless Network Has No Clothes.** http://www.cs.umd.edu/~waa/wireless.pdf

[14] Stubblefield A., Ioannidis J., D. Rubin A.,**Using the Fluhrer, Mantin, and Shamir Attack. to Break WEP. Revision 2,** August 21,2001, AT&T Laboroties and Rice University. http://www.uninett.no/wlan/download/wep_attack.pdf

[15] The iLabs Wireless Security Team, **What's wrong with WEP?,** Network World, 09/09/02. http://www.networkworld.com/research/2002/0909wepprimer.html

[16] R. Walker J., Intel Corporation, **Unsafe at any key size ; An analysis of the WEP encapsulation**, IEEE 802.11-00/345. www.dis.org/wl/pdf/**unsafe**.pdf

[17] The Wireless Ethernet Compatibility Alliance (WECA)'s response to the Berkeley Paper : **The Insecurity of 802.11.** http://www.packetnexus.com/docs/Wi-FiWEPSecurity.pdf

[18] Stuart J. Kerry et al, **Response from the IEEE 802.11 Chair on WEP Security**, IEEE 802.11 Working Group. http://slashdot.org/articles/01/02/15/1745204.shtml

[19] Potter, B.;**Wireless security's future,** Security & Privacy Magazine, IEEE, Volume 1, Issue 4, July-Aug. 2003 Page(s):68 – 72. http://ieeexplore.ieee.org/iel5/8013/27399/01219074.pdf?tp=&arnumber=1219074&isnumber=27399

[20] Housley R., **Alternate Temporal Key Hash,** IEEE 802.11-02/282r2 and IEEE 802.11-01/550r3. http://www.uninett.no/wlan/download/1-550.zip, and http://www.uninett.no/wlan/download/2-282.zip (Respectively)

[21] Ferugson N., **Michael: An improved MIC for 802.11 WEP.** http://www.uninett.no/wlan/download/2-020.zip

[22] Glenn F., Moskowitz R., **Weakness in Pass Phrase Choice in WPA Interface.** http://wifinetnews.com/archives/002452.html

[23] Altunbasak, H.; Owen, H.; **Alternative Pair-wise Key Exchange Protocols for Robust Security Networks (IEEE 802.11i) in Wireless LANs,** Southeast Con, 2004. Proceedings. IEEE, 26-29 Mar 2004 Page(s):77 – 83.

[24] Laverty D., **WPA versus 802.11i (WPA2):How your Choice Affects your Wireless Network Security.** http://www.openxtra.co.uk/articles/wpa-vs-80211i.php

[25] Cohen A., O'Hara B., **Introducing New Wireless Security.** http://www.pcworld.com/news/article/0,aid,110865,00.asp

[26] Wong S., **The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards.** http://www.sans.org/rr/whitepapers/wireless/1109.php

[27] Lane H. D., **Security Vulnerabilities and Wireless LAN Technology.** http://www.sans.org/rr/whitepapers/wireless/1629.php