A DISCUSSION OF WIRELESS SECURITY TECHNOLOGIES

Johanna Janse van Rensburg, Barry Irwin

Rhodes University

G01j202j7@campus.ru.ac.za,

b.irwin@ru.ac.za

(083) 944 3924

Computer Science Department, Hamilton Building, Rhodes University 6139

ABSTRACT

The 802.11 standard contains a number of problems, ranging from interference, co-existence issues, exposed terminal problems and regulations to security. Despite all of these it has become a widely deployed technology as an extension of companies' networks to provide mobility. In this paper the focus will be on the security issues of 802.11. Several solutions for the deployment of 802.11 security exists today, ranging from WEP, WPA, VPN and 802.11i, each providing a different level of security. These technologies contain pros and cons which need to be understood in order to implement an appropriate solution suited to a specific scenario.

802.11i provides a high level of security and must be used in scenarios where security is important. The recent 802.11i standard is discussed in detail and several of its vulnerabilities as identified by other researchers is evaluated in terms of the possibility of occurrence, risk and impact it has. For example, EAP is an intrinsic part of 802.11i; however several EAP methods contain security vulnerabilities, another factor to consider when setting up 802.11i for a WLAN.

Another common approach used to secure wireless networks are VPNs. Even though this appears as an attractive solution there are several issues which need to be considered before implementing it. If an organisation does not deploy a VPN already they will need additional technologies to do it. Another consideration is that VPNs' curb the throughput of a wireless network.

The old WEP and WPA standards cannot just be discarded because they have well known vulnerabilities. 802.11i was ratified in June of 2004, yet many institutes do not deploy 802.11i. Several reasons might exist; one is that the WLAN might not require a high level of security or that 802.11i is not understood.

It is no easy feat to provide a reliable, secure wireless solution while maintaining control and ensuring quality of service. This paper provides a holistic view of the security status of 802.11. This includes an understanding of the issues and pros and cons of each implementation. In order to provide readers with an understanding of how these technologies can aid in providing people with an efficient, reliable and secure network.

KEY WORDS

WEP, WPA, 802.11i, VPN

A DISCUSSION OF WIRELESS SECURITY TECHNOLOGIES

1 INTRODUCTION

With the popularity of 802.11 wireless technologies usage still growing, and the increased integration of this technology into organisational networks, the necessity for a secure wireless solution has been realised. Since the inception of 802.11 in 1999, [1] wireless security has evolved from Wired Equivalent Privacy (WEP) to Wi-Fi protected access (WPA) into a more mature solution, 802.11i. Not excluding the popular use of a Virtual Private Networks (VPN). Even now 802.11n is being developed as a standard [16]; with its advent it is sure to provide new challenges for WiFi.

WEP, WPA and 802.11i all attempt to provide confidentiality, integrity and authentication. However they do not all succeed at these tasks and introduce vulnerabilities into the WLAN's that implement them [1,7,10]. Therefore it is necessary to understand these weaknesses to be aware of the vulnerabilities which exist in a network where a specific technology is used.

In the following sections the weaknesses of WEP and WPA are discussed. Issues introduced by a VPN are examined. Furthermore 802.11i is discussed in detail. The 802.11i, WPA and VPN section will be discussed in more detail than WEP as the latter have gained extensive attention the past couple of years. Finally the advantages and disadvantages of each of these technologies are observed, in order to aid in making informed decisions on which security technology to map to a scenario.

1.1 WEP

Wired Equivalent Privacy (WEP) is a security protocol that was ratified with the IEEE 802.11 standard in 1999, and has since been replaced by 802.11i [1]. It attempted to provide authentication, confidentiality and integrity, but failed. Besides this fact it is still widely deployed, and therefore it is necessary to understand its vulnerabilities.

It is assumed that the reader has a basic understanding of WEP.

1.1.1 Key Management

WEP provides open-system or shared-key authentication. This shared key is also used to produce the cipher text for confidentiality. However a major problem of WEP is that it does not specify how to distribute the shared key which has led to an abuse of this model. If the shared key is found it will compromise the confidentiality of a conversation. It is left to the users and the network administrators to ensure the safe distribution of keys. Often the key does not get changed for long periods of time, this result in several vulnerabilities introduced into the system. These vulnerabilities include duplicate and static WEP keys, factory defaults and weak keys [1,2]. From these the shared key can easily be deduced.

1.1.2 Key stream re-use attack

WEP is based on the RC4 algorithm. Its implementation in WEP has proven to be insecure, and vulnerable to a key stream re-use attack. This attack occurs when the same key stream or partial key stream is used in the XOR operation. Identical plaintexts XORed with the same key-stream will result in identical cipher texts. It is surprising how often certain texts are repeated. For example passwords and log-in prompts are consistent amongst users and the fields in IP traffic are identical. The XOR of two cipher texts will result in the XOR of their plaintext [3].

```
C1 XOR C2 = P1 XOR P2
```

An Initialisation Vector (IV) was built-in to prevent these attacks from happening, but failed. The 24-bit field used by the IV is too small and can be exhausted in a matter of a few hours. As a result the IV will repeat itself in a busy network. Since key management is a problem in WEP the key does not change. The combination of a reused IV and unchanged key results in the same key stream to be used. Furthermore these IVs are easily detected as they are sent in plaintext [3].

1.1.3 Integrity

WEP uses CRC for integrity. It was originally used for error detection and was not designed for data integrity. The function used in CRC 32 is linear which means that a bit changed in the text can be propagated to the checksum. Consequently an attacker can change bits in the cipher-text, change the checksum accordingly and the change will not be detected [3].

1.1.4 Rogue Access Point

WEP uses a one way authentication scheme where the access point is not authenticated to the mobile station [2]. This makes the WLAN vulnerable to rogue access points. For example an adversary can spoof itself as an AP and gain access to all the information of the client that connects to it [4].

WEP is easy to implement and does not require any extra hardware. However well known weaknesses in WEP have been identified and tools have been written which exploit these vulnerabilities with relative ease. Besides these vulnerabilities it will deter casual eavesdropping. A WEP implementation will be viable if the information exchanged on the WLAN are not important, and has a low risk if exposed.

2 VIRTUAL PRIVATE NETWORKS

Once the weaknesses in WEP were known institutions turned to Virtual Private Networks (VPN) as add on security mechanism. VPN technology was originally designed to provide a secure connection to mobile users connecting to an intranet over a public external network. VPN networks have various roles [6]:

- Connecting branches of the same organizations in physically different locations securely together.
- Connecting business partners.
- Allowing mobile users to access company resources from physically remote locations.

A VPN creates a tunnel on top of a protocol. Various protocols exist to be used with VPN’s, these are listed below [6]:

- Point to point tunnelling protocol (PPTP) - A tunnelling protocol licensed to Microsoft.
- Level two transport Protocol (L2TP)
- IP Security (IPSec) - Operates at the Network layer i.e. OSI layer three. IPSec needs client software installed on devices to be able to connect to the company private networks. Hence each wireless client must have this software installed. IPSec is the better solution for connecting two private networks together over the Internet. Keep in mind that due to the fact that different vendors implement different implementations of IPSec it lacks interoperability.
- Secure Socket Layer (SSL) operates at the Application layer and encrypts all HTTP enabled applications. Therefore an application must be HTTP enabled to use this solution. SSL is a better solution to be used with remote users to connect to private networks.

A wireless user simply acts as a mobile user connecting to the internal network from outside. The transactions of the wireless user are handled in exactly the same way as a mobile user connecting over a public external network. This provides a secure connection to a wireless client using the VPN [6].

IPSec and SSL is the focus in this section. If the wireless client applications use HTTP then an SSL approach will do, however if the user applications do not use HTTP then IPSec is preferable [5].

A VPN encrypts data traffic at the upper layers, this means that layer two traffic is unencrypted, which is where wireless networks broadcasts. This is one of the drawbacks of using a VPN solution. For example IPSec uses layer three to transmit and SSL layer four; this could possibly create a security hole, as data link information such as packet headers are easy to sniff [22].

Interoperability is another issue with VPN technologies, as the different vendor technologies do not work together. This is another issue to consider when choosing a VPN implementation. Furthermore a VPN will reduce the throughput of a network by 15%. This is as a result of the strong encryption, tunnelling and the packet overhead of a VPN [6].

VPNs offer improved security from WEP. However it was not designed for wireless networks and has a negative effect on the overall throughput. This could be a good solution if a network already implements a VPN as the wireless network would be an extension. But if the company does not it will mean acquiring additional hardware. In this case it might be better to go for the security that WPA or WPA2 has to offer. In other words the security provided by the 802.11 standard.

3 ROBUST SECURITY NETWORK

A crucial part of WiFi Protected Access (WPA) and 802.11i wireless security involves understanding the Robust Security Network (RSN) framework, therefore this is discussed first before WPA and 802.11i are examined.

With the development of 802.11i the IEEE developed a new security architecture for WLANs called the *Robust Security Network (RSN)*. The RSN framework negotiates algorithms to be used for communication between Access Points (APs) and clients, enabling new authentication and encryption algorithms to be used as new threats are discovered [7]. RSN defines three elements depicted in Figure 1 [7]:

- Supplicant—The client that wants to connect to the network;
- Authentication Server—For example a RADIUS server.
- Authenticator—The access point which passes messages between the client and the authentication server, it does not do any authentication;

The IEEE 802.1x standard is used to implement this.

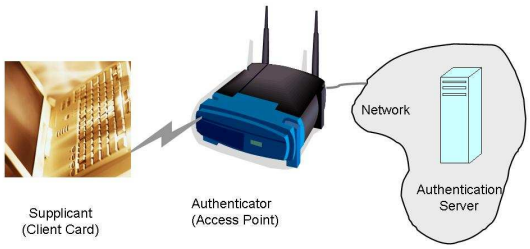

Figure 1, The entities that comprises the RSN [8]

3.1 Extensible Authentication Protocol (EAP)

EAP is the protocol used by the above three entities to communicate during the authentication process. EAP supports multiple authentication mechanisms, for example digital certificates, challenge response tokens and passwords [8]. The authentication protocols used get encapsulated within the EAP messages. The EAP messages consist of four messages, as depicted in figure 2, *Request, Response, Success* and *Failure.* Once a Supplicant has received a *Success* message, it has been authenticated to the authentication server and the message protection process follows [8].

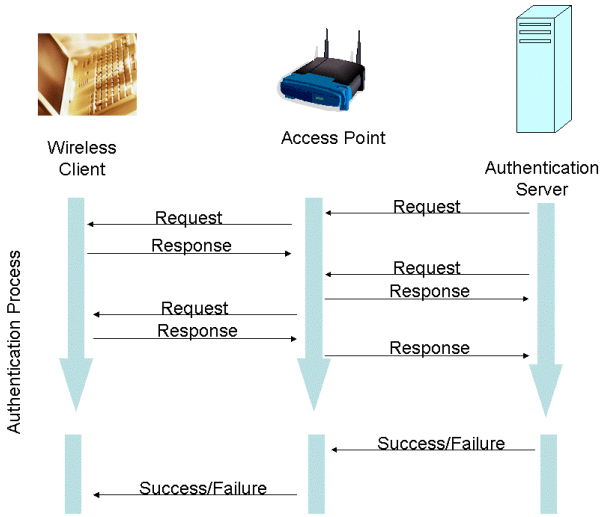

Figure 2. The authentication methods are encapsulated within the above messages. These can be tunnelled, public key or secret key approaches [8].

One must be careful of the authentication protocols used with EAP as some methods are insecure. For example the LEAP implementation developed by CISCO is vulnerable to dictionary attacks as is Kerberos [8]. 802.11i has requirements which an EAP method needs to adhere to before it can be accepted as a valid authentication process; these can be seen at RFC 4017. A few of these are [12]:

- The EAP method must generate symmetric keying material.
- It must generate a key with at least 128bit strength.
- It must support mutual authentication.
- It must be resistant to dictionary attacks.

Once the supplicant has been authenticated, and a shared key established, a session bound Pairwise Master Key (PMK) is generated and sent via a secure connection to the AP from the authentication server. From this key a Pairwise Transient Key (PTK) gets generated during the four-way-handshake [9]. As depicted in Figure 3. The PTK gets divided into three keys [11].

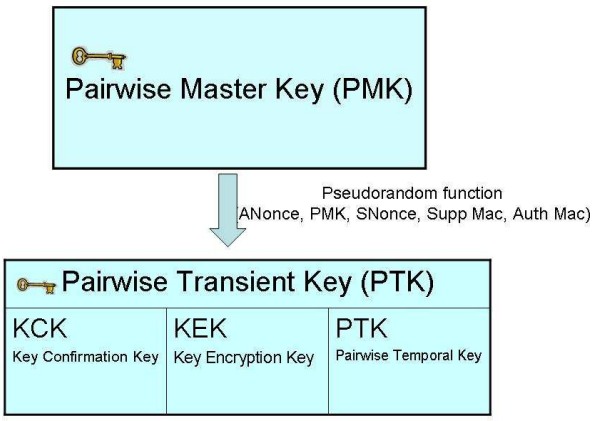

Figure 3 Key hierarchy [11]

- Key confirmation key (KCK) - It is used to provide authentication of the origin of data in the four-way-handshake and group key handshake messages.
- Key encryption key (KEK) – This key gets used to provide confidentiality in the four-way-handshake and group key handshake messages.
- Pairwise temporal key (PTK) - It is used by the data confidentiality protocols.

Alternatively for SOHO users who do not have an 802.1x server a Pre Shared Key (PSK) can be used to generate the PTK. A PSK can be a pass phrase between 8 to 63 bytes long or a 256 bit number [10].

3.2 Four-way-handshake

The four-way-handshake verifies the cipher suite for a particular session. On the successful completion of the four-way-handshake the PTK is established [11]. As its name implies it consist of four messages executed in sequence. These messages are explained below [11].

1. In the first message the authenticator send a message to the supplicant with the nonce known as the ANonce. This information is used by the supplicant with the previously negotiated PMK to calculate the PTK.

2. The supplicant generates its nonce, the Snonce and calculates the PTK, with a Pseudo Random Function. The following parameters are used in the calculation, Supplicant and Authenticator MAC address, Snonce, Anonce and PMK. It sends the Snonce and security parameters used during association to the authenticator. The MIC gets calculated with the KCK. It is used by the authenticator to verify the message information.

3. In this message the security parameters of the authenticator send in its Beacon Frames are sent to the supplicant. The Group Temporal Key (GTK), used to encrypt broadcast traffic, is encrypted with the KEK and sent. Once again a MIC of the message is calculated.

4. The last message indicates that the temporal keys have been established and can now be used by the data confidentiality protocols.

By re-sending the security parameters used during the initial association the supplicant confirms that the parameters negotiated during the association process are valid [7].

With the background knowledge gained from this section, the following sections will explain how WPA and 802.11i security works, and the weaknesses they possess.

4 WIFI PROTECTED ACCESS (WPA)

WPA superseded WEP in 2003, however it is not a standard. It was created by the IEEE and WiFi-Alliance as a temporary solution to the weak security provided by WEP and was designed to work with old legacy WiFi equipment [13].

Encryption is provided by the Temporal Key Integrity Protocol (TKIP) [13]. Authentication is provided by 802.1x EAPOL. Integrity is checked by the Michael algorithm. WPA still uses RC4 but larger 48bit key IV is used which takes a long time to repeat [13].

It provides two options of implementation: one to enterprise users the other to small office home office (SOHO) users. The enterprise solution makes use of an 802.1x server. The SOHO deployment uses a pre-shared key (PSK) as an alternative to 802.1x. A PSK can be a pass phrase between 8 to 63 bytes long or a 256 bit number [10].

WPA attempts to fix the problems encountered with WEP. This section discusses how WPA solved some of the WEP problems and the flaws which still exist.

4.1 TKIP (“tee-kip”)

TKIP was developed with WPA to improve on WEP. It attempts to eliminate a key stream re-use attack. In order to provide backward compatibility TKIP still uses RC4 but improves the encryption by scrambling the keys. For each packet sent over the network it generates a new key, or temporal key [13]. However the temporal key is based on the original shared key and hence the security is dependant on how well the shared key is kept a secret.

4.2 Rogue Access Points

Unlike WEP, WPA provides mutual authentication with 802.1x as both the supplicant and the authentication server gets authenticated to each other through the EAP method used. This prevents the client from connecting to “rogue” access points [13].

4.3 Key Management

WPA provides key management through 802.1x. After the client and authentication server are authenticated, the authentication server creates a master TKIP which is sent to the client, and via a secure connection to the authenticator [13]. With each authentication a new master key gets generated, this replaces WEP static keys problem. The four-way-handshake between the authenticator and supplicant follows and the keys are installed [13].

4.4 Integrity

Integrity is provided by the Michael algorithm. The supplicant and authenticator use a strong mathematical function to calculate the message integrity check. If these do not match the message is discarded [13].

4.5 DoS attack

The EAP-Start, Logoff and failure messages used by 802.1x are not protected. An adversary can easily forge these messages. For example by flooding the network with forged EAP-Logoff

messages clients will never be able to connect to the network which will cause a DoS. This vulnerability exists for both WPA and 802.11i [7].

4.6 PSK Weakness

This weakness is similar to that of the key stream re-use attack of WEP. One of the weaknesses in WPA and 802.11i is the option to use a Pre Shared Key (PSK) which is shared amongst all the users of the network [10]. The PSK can be provided in the form of a 256 bit number or a pass phrase. In the case of a pass phrase it can be converted to a PMK using a simple formula [10].

```
PMK = PBKDF2(passphrase, ssid, ssidLength, 4096, 256)
```

The SSID is easy to obtain, therefore in order for an attacker to calculate the PMK only the passphrase needs to be obtained. It is recommended by the WiFi alliance to have a passphrase of at least 20 characters long. Anything less is considered to be insecure and subject to a dictionary attack [10]. Another weakness is that if the master key is shared amongst peers they have the ability to eavesdrop on each other [17].

As explained above the PTK is derived from the PMK. The parameters used to generate it, include the Snonce, Anonce and MAC addresses of the supplicant and the authenticator. These parameters are easy to obtain with a simple tool like ethereal, hence if the PSK is known the whole key hierarchy can be derived [14].

One such tool which exploits this weakness is coWPAtty. It first needs to obtain a four-way handshake and then attempts to guess the PSK by attempting a brute-force attack on the key [14]. WPA requires the use of additional hardware, like the RADIUS server.

However the option to use a PSK was provided for SOHO users with a small network. Even though hacking tools that exploit WPA vulnerabilities exists the skill level required to do so is higher.

802.11i

The IEEE 802.11i standard was ratified in June 2004. It is similar to WPA but with a number of improvements. The security mechanisms used by the 802.11i standard are discussed below.

4.7 Association

Before the authentication process ensues association takes place. During this step the security parameters which will be used between the supplicant and authenticator for a particular session are negotiated. Even though this process is insecure it will later be secured during the four-way-handshake [11].

4.8 Authentication

As with WPA, 802.1x is used for the authentication process, during this process both the authentication server and supplicant gets authenticated to each other. 802.11 uses EAP over LAN (EAPOL) key frames for the exchange of information between the supplicant, authenticator and authentication server [9]. The four-way-handshake is performed for key management and to finalise the authentication. By generating the keys during the four-way handshake 802.11i provides automatic key management, a feature which lacked from WEP [11].

4.9 Confidentiality

802.11i uses the Cipher Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) and TKIP for the data confidentiality protocol. CCMP is computationally intensive and could not be run on legacy wireless equipment therefore TKIP was included to provide backward compatibility. CCMP provides packet authentication as well as encryption [11]. Following, is an explanation of the building blocks of CCMP.

CCMP uses the Counter with CBC-MAC (CCM) operation mode of the Advanced Encryption Stadard (AES) algorithm to provide confidentiality [7]. Cipher Block Chaining (CBC) is a frequently used block cipher mode, in other words it can be used with any block encryption algorithm [15]

MAC or message authentication code ensures that a message has not been tampered with [23]. MACs have a secret key only known to the sender and the receiver. A MAC function is run over a message to compute a MAC value. This value is attached to the message before sending it. The receiver calculates the MAC from the message and compares it with the attached MAC value. If they do not match it will discard the message. CBC-MAC turns a block cipher into a MAC. For authentication and integrity CBC-MAC gets used [11].

Counter (CTR) mode is another block cipher encryption mode. It is a stream cipher, which generates the key stream by concatenating the nonce with the counter value and encrypts it to form the keystream [23]. AES is a block cipher operating on blocks of data 128 bits long. It is considered to be a safe encryption scheme.

4.10 DOS

Another vulnerability which exists for WLANs are DOS attacks. This is because the management and control frames of 802.11b are not protected. For example an attacker can forge the Deauthentication or Disassociation messages, which will kick a client off a WLAN [7]. In addition, a flood of association requests may be sent to an AP, preventing any other client from connecting to the AP [17].

Yet another weakness is that of the virtual carrier sense method. By forging a Request to send (RTS) message, providing the Network Allocation Vector (NAV) with an exceptionally big value other devices will consider the channel busy and back-off, resulting in the suppression of their transmissions [7].

A successful DOS attack might lead to more advanced attacks, like a man in the middle attack [7]. It appears as if the 802.11i standard does not sufficiently make provision against a DOS attacks.

802.11i defines a Transient Security Network (TSN) which provides backward compatibility with legacy equipment. This allows for the co-existence of both RSNA and Pre-RSNA algorithms [9]. Such a mix lowers the level of security to that of the weakest algorithm. If this approach is used the administrator must keep this in mind.

It is recommended that 802.11i be used when sensitive data needs to be secured. Only a few of the vulnerabilities in 802.11i are discussed. Even though attacks exist on 802.11i they require a high skill level and it is not probable that they will be executed. To date there are no tools that can be used to exploit 802.11i vulnerabilities. Therefore it is only the skilled and determined attacker who will attempt to break into an 802.11i network.

5 OTHER WEAKNESSES

With the advent of WPA and the introduction of RSN a lot of the security problems from WEP have been solved. However there still remain some problems. The following two attacks are relevant to both 802.11i and WPA. It focuses on the weaknesses of the implementation of the RSN framework.

5.1 Man in the Middle Attack

As mentioned earlier 802.1x in conjunction with EAP attempts to provide a framework in which the supplicant and authentication server mutually authenticate each other. However as depicted in Figure 2 it can be seen that a *Success* message is only send from the authentication sever to the

supplicant and not from the supplicant to the authentication server. Therefore an attacker could forge a *Success* message to the supplicant posing as the authenticator, giving the attacker access to the network traffic exchanged between the supplicant and the authentication server. Even though the authentication protocol executed within the EAP exchange performed mutual authentication a Man in the Middle Attack (MIM) might still be possible [18].

However RFC 3748 seem to address this vulnerability. An EAP authenticator (authentication server) is only allowed to send a *Success/Failure* messages once the whole authentication process of the authentication protocol has completed. If a *Success* message is received prior to this point, the supplicant must discard the message, this also holds when a supplicant receive a message immediately after it connects. This provision has been brought into place to prevent an attacker to perform a MIM attack [19].

5.2 Session Hi-Jacking

Mishra *et al* explains the possibility of a Session Hi-Jacking with the 802.1x standard. This occurs after a supplicant has received an authentication message from the authenticator, who is now in the authenticated state. An attacker spoofs the MAC address and sends a disassociation message to the supplicant, who is then in the disassociated state. Conversely the authenticator still considers the supplicant as authenticated. The attacker can spoof the MAC address of the client and continue the session, because the authenticator never disassociated the supplicant [18]. This could only work in a network where encryption is not enabled; otherwise the attacker will not be able to talk to the access point.

6 CONCLUSION

Wireless related technologies have evolved at a rapid rate the past couple of years. Finally a mature security solution, 802.11i has arrived. It is regarded by some to be even more secure than wired security [20]. 802.11i was inaugurated in June 2004. In a 2005 survey done WLANs 22% of respondents claim to implement 802.11i and 42% use VPNs. Even though over a third of the respondents state that they feel wireless security has been solved 24% do not feel confident about implementing a security solution. Security remains the top-ranking challenge to overcome when implementing a WLAN [21].

In this paper the wireless security technologies and their relevant vulnerabilities are summarised. In appendix A, a table of the above discussed vulnerabilities are given to compare which security technology is vulnerable to each. The purpose of this paper is to provide the ability to make an informed decision about the security technology required when implementing a WLAN.

7 REFERENCES

[1] Gast Matthew S. 802.11 *Wireless Networks: The Definite Guide*. 1st ed O'Reily, 2002.

[2] T. Karygiannis and L. Owens. Wireless Network Security 802.11, Bluetooth and Handheld Devices. *NIST SP 800-48 National Institute of Science and Technology*. November 2002

[3] N Borisov, I. Goldberg and D. Wagner. Intercepting Mobile Communications: The insecurity of 802.11 *In Proceedings of the 7th annual international conference on Mobile computing and networking*, July, 2001

[4] P. Chandra. 802.11 Security May 2002 http://www.wirelessdevnet.com/articles/80211security/

[5] R Stanton. Securing VPNs: comparing SSL and Ipsec *Computer Fraud & Security, Volume 2005, Issue 9, Pages 17-19,* September 2005,

[6] K.S. Munasinghe VPN over Wireless Infrastructure: Evaluation and Performance Analysis. *Thesis University of Western Sydney.* March 2005

[7] C. He and J.C. Mitchell, Security Analysis and Improvements for IEEE 802.11i, *Network and Distributed System Security Symposium (NDSS '05)*, February, 2005.

[8] K. H. Baek, S W. Smith, and D Kotz. "A Survey of WPA and 802.11i RSN Authentication Protocols." *Darmouth college Computer Science Technical Report* November 2004

[9] IEEE Standard 802.11i-2004 Information Technology – Telecommunications and Information exchange between systems – Local and metropolitan area networks – Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical (PHY) specifications.

[10] R. Moskowitz. Weakness in Passphrase Choice in WPA Interface. November 2003 http://www.wifinetnews.com/archives/002452.html

[11] D Halasz. IEEE 802.11i and wireless security. August 2004. http://www.embedded.com/showArticle.jhtml?articleID=34400002

[12] D. Stanley, J. Walker and B. Aboba. Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs. *RFC4017*, March 2005

[13] Wi-Fi Alliance. Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks. www.wi-fi.org 2003

[14] S. Fogie. Cracking Wi-Fi Protected Access (WPA) http://www.informit.com/articles/article.asp?p=369221 March 2005

[15] B. Pawliw. Security Definitions – cipher block chaining. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci344945,00.html October 2000

[16] J. M. Wilson. Quadrupling Wi-Fi speeds with 802.11n. http://www.deviceforge.com/articles/AT5096801417.html August 2004

[17] L. Phifer. Risky business: Understanding Wi-Fi threats. http://businessweek.bitpipe.com/detail/RES/1144266249_509.html. Nokia – Webcast. April 2006

[18] A Misra, W.A. Arbaugh. An initial Security Analysis of the IEEE 802.1X Standard. University of Maryland. February 2006

[19] B. Aboba, L. Bunk, J. Vollbrecht, J. Carlson, H. Levkowetz. Extensible Authentication Protocol. *RFC3748*, June 2004

[20] B. Posey. Have Wireless Networks Surpassed the Security of Wired Networks. http://www.windowsecurity.com/articles/Wireless-Networks-Surpassed-Security-Wired-Networks.html. March 2005

[21] J. Wexler. Wireless LAN State-of-the-Market Report. http://www.webtorials.com/abstracts/WLAN2005.htm. April 2005

[22] By J. L. Bindseil, Tightening Wireless LAN Security, Symantec http://www.ebcvg.com/articles.php?id=270 October 2004

[23] N. Ferguson and B. Schneier, Practical Cryptography, *John Wiley & Sons*, 2003

8 APPENDIX

Table 1 In this table possible attacks are listed compared to the security technologies

Are the below attacks possible?	**WEP**	**WPA**	**802.11i**
Session Hijacking	Yes	Enterprise - No PSK – Possible	No
Man in the Middle	Yes	No PSK – Possible	No
DOS protection	No	No	No
Rogue AP protection	CRC32 – Failed	No	No
Confidentiality	RC4 – Failed	TKIP – Better	CCMP – Success
Key-Stream Replay attack	Yes	No But PSK vulnerable	No
Passive Eavesdropping	Yes	No	No
Traffic Injection	Possible	No	No
Are Mutual Authentication provided?	No	Yes	Yes
Are Key Management provided?	No	Yes	Yes

9 ACKNOWLEDGEMENT

This work was undertaken in the Distributed Multimedia Centre of Excellence at Rhodes University, with financial support from Telkom SA, Business Connexion, Comverse, Verso Technologies, Tellabs and StorTech THRIP, and the National Research Foundation.