ISSN:2320-0790

An International Journal of Advanced Computer Technology

SECURITY THREATS ANALYSIS OF WIRELESS LOCAL AREA NETWORK

[1]Clement Agbeboaye, [2]France O. Akpojedje, and [3]Joshua Okoekhian

[1,2,3]Department of Electrical and Electronic Engineering Technology,
National Institute of Construction Technology (NICT), Uromi, Nigeria.

Abstract: There is a geometric growth in the manufacturing and sales of wireless network devices presently. This growth is not connected with the advantages ushered in by wireless network e.g user mobility, the flexibility of the network, enable network connection for different kinds of devices, increased productivity, etc. However, because the wireless network is broadcast in nature, it has numerous security challenges, if these security challenges are not addressed, different attacks can be lunged against the network such as theft of data, unauthorized access to the network, denial of service, etc. These security challenges are caused majorly by the body implementing the data confidentiality protocol and the wireless device users. Nowadays, almost all wireless access points (APs) are secured with Wi-Fi Protected Access 2 (WPA2) because hitherto WPA2 is known to provide the highest form of security to wireless local area network (WLAN). Consequently, we investigated various wireless network security protocols, focusing more on WPA2 since it is the latest amongst the protocols. Real-time dictionary attack against WPA2 was carried out to prove the existence of flaws in the protocol. Hence, countermeasures were proposed to forestall these flaws in the system and; if the suggested measures are implemented, it will lead to the development of a more secure wireless network.

Keywords: Network Security, Security Protocols, Wireless Network, WPA2, Wi-Fi, Network Attacks

I. INTRODUCTION

Wireless Network is becoming more popular every day. This is a function of the advantages associated with it. Such advantages include ease of network configuration and reconfiguration, increased accessibility to information resources [1], mobility support and roaming which grant the users "anytime," anywhere access to network [2]. Wireless network security is more concentrated and complex than security of wired networks because wireless signal is broadcast in nature, making it possible for anyone within the range of a wireless device to intercept the packets sent without interrupting the flow of data between the wireless device and the access point [2]. Some of the security threats in Wireless Network are: Man-in-the-middle (MitM) attack, Denial of service attack, sniffing, rogue access point, replay attack, etc. With the help of a wireless device and some applications, these attackers can gain access to the wireless network unlike the wired equivalent. This is mostly because wireless network is radiated into free space (available to all wireless devices). The aim of these attackers could be to gain unauthorized access to internet service which could affect the overall throughput or performance of the network, unauthorized access to files in victim's Computer, injection of malicious packets into the network, monitoring of packets flowing in the network, etc.

In order to mitigate these security threats associated with wireless network, Wired Equivalent Privacy (WEP) encryption was introduced in the year 1999, "to try to solve the problems of protection of wireless local networks similar to the protection level of wired local networks" [3]. Unfortunately, WEP encryption is no longer considered secure because tools such as Airsnort or Aircrack can quickly recover its keys [4]. As a result of WEP's weakness, the Wi-Fi Alliance approved Wi-Fi Protected Access (WPA) which uses Temporary Key Integrity Protocol (TKIP) [4]. Soon,

a flaw was detected in WPA which makes it vulnerable to attacks. Wi-Fi Protected Access 2 (WPA2) encryption was introduced in 2004. Till date, WPA2 provides the highest level of security for the wireless networks by eliminating most of the security flaws in WEP and WPA, and providing 128bits encryption security for wireless networks [2]. WPA2 has been known to be very secure for a long time until recently in October 2017, it was discovered that there are some design flaws in the encryption protocol. The vast majority of our Wireless Networks are secured using WPA2. If WPA2 which is universally known to be the dominant wireless encryption protocol have some loopholes, it means there is a global security threat to Wi-Fi network. In this paper, our major focus is the design flaws in WPA2 since it provides the highest level of security to our Wi-Fi Network. We investigated the security issues in WPA2, analyze the weaknesses in the protocol and present a reverse engineering countermeasure to correct or ameliorate these flaws. Hence, the remaining parts of this paper is structured as follows: Section 2.0 introduces related work, section 3.0 overview of four (4) handshake, section 4.0 materials and methods, section 5.0 dictionary attack against WPA2 protocol, section 6.0 countermeasures and section 7.0 conclusion and recommendations.

II. RELATED WORK

Since wireless signal is radiated into free space which is readily available to any wireless device within the range of the network, wireless network security is a very big challenge nowadays. As a result of this security challenge, IEEE released different protocols at different time to increase the security in Wireless Network. Different security protocols and Encryption standards are discussed below.

2.1 Wired Equivalent Privacy WEP

Wired Equivalent Privacy (WEP) was introduced in the year 1999 to enhance the security (confidentiality, integrity and availability) of information flowing along the network.WEP is based on the RC4 encryption algorithm with a secret key of 40 bits or 104 bits being combined with a 24-bit Initialization Vector (IV) to encrypt the plaintext message and its checksum – the ICV (integrity check value) [6]. Figure 1 below is an example of a basic WEP encryption.

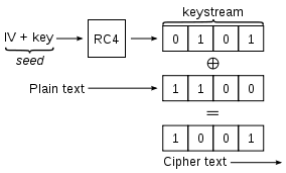


Figure 1: Basic WEP encryption: RC4 Keystream XORed with plaintext [5].

However, in August 2001, Scott Fluhrer, Itsik Mantin and Adi Shamir Published a Cryptanalysis of WEP that exploits the way the RC4 Ciphers and IV are used in WEP, resulting in a passive attack that can recover the RC4 key after eavesdropping on the network as little as one minute[6]. As a result of the flaws associated with the protocol, it is not recommended to use WEP.

2.2 Wi-Fi Protected Access (WPA)

In order to curb the shortcomings of WEP, in October 2003, the Wi-Fi Alliance introduced Wi-Fi Protected Access (WPA) security protocol. The WPA standard employs Temporal Key Integrity Protocol (TKIP) for encryption, using 128 bit keys that are dynamically generated [7]. However, WPA was designed to temporarily take care of the inherited WEP vulnerabilities and the fact that some parts of TKIP (like Michael) possesses known security relevant flaws, WPA cannot be assumed to be secured in the long run [4].

2.3 Wi-Fi Protected Access 2 (WPA2)

The Wi-Fi Alliance Certified systems in compliance to IEEE 802.11i's Robust Security Network Association (RSNA) developed an algorithm, Counter-Mode-CBC-MAC (CCMP) under the name Wi-Fi Protected Access 2 (WPA2) [8]. In WPA2, the RC4 algorithm encryption was replaced with Advanced Encryption Standard (AES). With one single 128-bit AES key, one is able to encrypt all packets, eliminating the key management problems of WEP and TKIP [4]. This system of Wi-Fi encryption was introduced in 2004. WPA2 has been known to be very secure for a long time until recently in October 2017, it was discovered that there are some design flaws in the encryption protocol. All Wi-Fi networks that are protected use the 4-way handshake to generate a fresh session key [9] for encryption and decryption. Marthy Vanhoef in [9] was able to demonstrate that the 4-way handshake and other handshakes are vulnerable to key reinstallation attack. In his work, he showed that when a client joins a network, it executes the 4-way handshake to negotiate a fresh session key. This key will be installed after receiving message 3 of the 4-way handshake. After the installation of the key, normal data frames will be encrypted by it using a data confidentiality protocol. Nevertheless, because messages may be lost or dropped, the Access Point (AP) will retransmit message 3 if it did not receive an appropriate response as acknowledgement. Thus, the client may receive message 3 several times. Every time it receives this message, it will reinstall the same session key and thereby reset the incremental transmit packet number (nonce) and receive replay

counter used by the data confidentiality protocol. He showed that an attacker can force these nonce resets by collecting and replaying retransmissions of message 3. By forcing nonce reuse in this manner, the data confidentiality protocol can be attacked e.g. packets can be replayed, decrypted and/or forged. If WPA2 which is known to have the highest level of security in our wireless fidelity network has some design flaws, technically it means our Wi-Fi network is open to serious danger.

III. OVERVIEW OF THE 4-WAY HANDSHAKE

The 4-way handshake provides mutual authentication based on a shared secret called the Pair wise Master Key (PMK) and negotiates a fresh session key called the Pair wise Transient Key (PTK) [9]. The duration for the PMK is for an entire session thus it should not be disclosed to a third party. The two parties involved in this authentication is the AP also known as the Authenticator and the Client also known as the Supplicant. Concatenating the PMK, Authenticator Nonce (ANonce), Supplicant Nonce (SNonce), the Authenticator MAC address and the Supplicant MAC address derive the PTK. After deriving the PTK, it is divided into Key Confirmation Key (KCK), Key Encryption Key (KEK) and Temporal Key (TK). The KCK and KEK are used to protect handshake messages while the TK is used to protect normal data frames with a data confidentiality protocol [9]. In a 4-way handshake, four (4) messages are sent between the Access Point (AP) and the Client (Wireless Device). Message 1 is sent from AP to the client. It contains MAC address of AP (AA), the incremental transmit packet number (ANonce) chosen by AP and a replay counter (SN). Message 1 is not encrypted because the PTK was not derived as at the time it was sent. After receiving message 1, the Client generate its MAC address (SPA) and incremental transmit packet number (SNonce). Thus, the PTK is derived from the parameters mentioned in the paragraph above after the Client received message 1. Message 2 is sent from the Client to the AP. With the help of the Message Integrity Protocol (MIC), the AP is able to verify if it has the same PTK as compared to the one derived by the client. Message 3 is similar to message 2 but in this case, the AP add a Group Temporal Key (GTK). The GTK is used to protect broadcast frames in the network. On receiving message 3, the Client sends message 4 which serves as acknowledgement to the AP. Figure 2 below is a representation of the 4-way handshake.

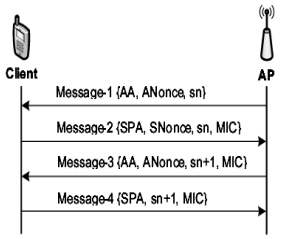


Figure 2: Four (4) Way Handshake in 802.11i [10].

IV. MATERIALS AND METHODS

The data used for this study was obtained from a mobile phone Wi-Fi network which serves as our Wireless Local Area Network (WLAN). In order to ascertain the security of wireless LAN, dictionary attack against WPA2 protocol was carried out.

To carry out this attack successfully, we downloaded and installed Kali Linux application from their website. All the tools and sub-tools required to carry out the attack mentioned above were all present in the application. However, for the successful download, installation and proper functioning of Kali Linux, there are some certain requirements that must be met by the computer system (Laptop) we intended to use for the attack. These requirements are:

a) A minimum of 20GB disk space for the Kali Linux installation.
b) RAM for i386 and amd64 architectures, minimum 1GB or more.
c) CD-DVD/USB boot support.
d) A wireless network adapter that supports monitor mode and packets injection e.g Alfa AWUS036NEH 2.4GHz, Panda PAU05 2.4GHz, etc.

If these minimum requirements are met, Kali Linux can be downloaded into the Laptop. It should be noted that the sampled study for this research is applicable to any wireless LAN in the whole world. The data obtained for the dictionary attack is presented in section 5.0 below.

V. DICTIONARY ATTACK AGAINST WPA2 PROTOCOL

To carry out a Dictionary attack against an AP with WPA2 security protocol, the following terminal program on Kali Linux were run: Open a terminal and run iwconfig. This is done to know the name of the wireless interface of the computer. In this case the name of the wireless interface is wlan0.

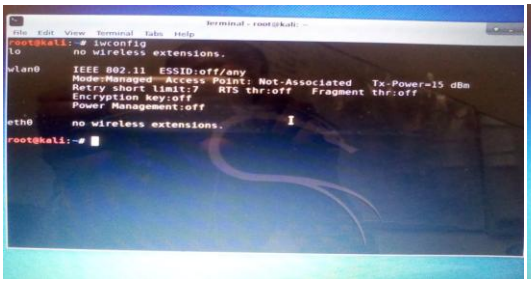


Fig. 3

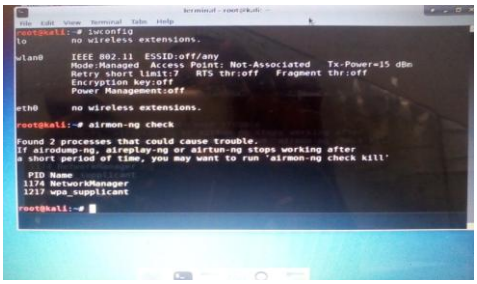


Fig. 4

Figure 3: Steps to carryout Dictionary attack against WPA2 (One)

Next, run "airmon-ng check," this is done to know if there is any process that can cause trouble to the procedure.

Figure 4: Steps to carryout Dictionary attack against WPA2 (Two)

In this case, two processes were found that can cause trouble. Then run "airmon-ng check kill" to kill the processes.

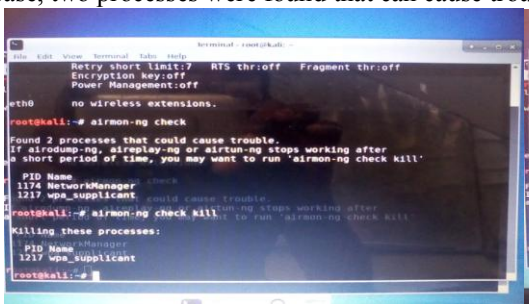


Fig. 5

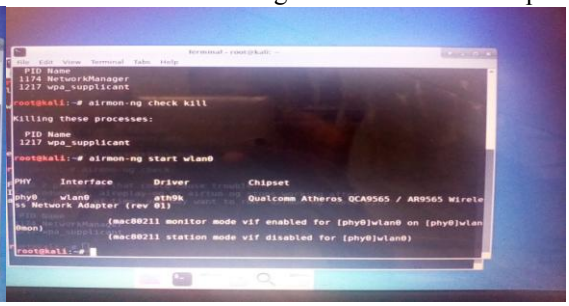


Fig. 6

Figure 5: Steps to carryout Dictionary attack against WPA2 (Three)

Then run "airmon-ng start wlan0", this is done to set the wireless network interface card to monitor mode.

Figure 6: Steps to carryout Dictionary attack against WPA2 (Four)

Here, the wireless network interface card is set to monitor mode and the wireless interface is changed from wlan0 to wlan0mon.

Then run "airodump-ng wlan0mon" to monitor the available Wi-Fi network in that location. It displays the APs in that location and the clients connected to the various APs. It also displays a lot of information such as BSSID, Stations, ESSID, Channels, etc.

Fig. 7

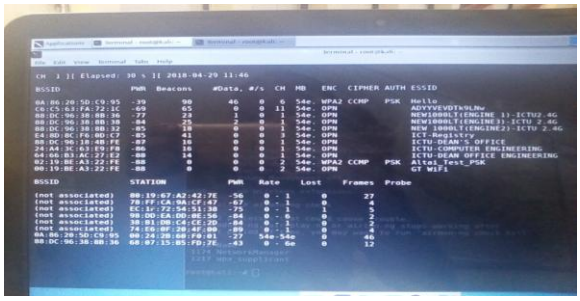


Fig. 8

Figure 7: Steps to carryout Dictionary attack against WPA2 (Five)

Then the various devices connected to the various APs are displayed below.

Figure 8: Steps to carryout Dictionary attack against WPA2 (Six)

Here, the available APs and the clients connected to them were displayed. Note that two APs were encrypted with WPA2 but others were opened. We decided to launch a Dictionary attack on the AP with ESSID "Hello."

Before launching the attack, we need to run channel 6 with airodump-ng where the ESSID "Hello" is located. Thus, press Ctrl+C to stop the previous process and run "airodump-ng –c 6 –a 0A:86:20:5D:C9:95 –w /root/Desktop/capture wlan0mon."
Here:

i. -c stand for channel
ii. 6 is the channel of the AP "Hello"
iii. -a stand for the BSSID
iv. 0A:86:20:5D:C9:95 is the MAC address of the AP
v. -w is used to write the captured packets to a specified path, in this case it is /root/Desktop/capture wlan0mon

The command above displays this terminal below.

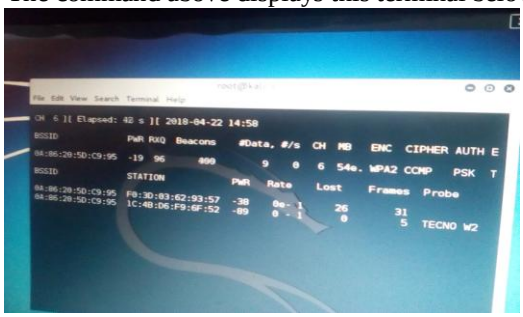


Fig. 9

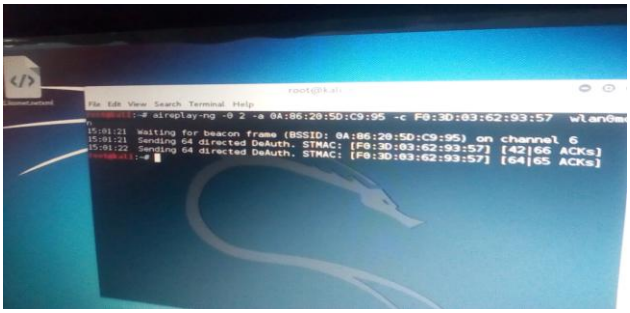


Fig. 10

Figure 9: Steps to carryout Dictionary attack against WPA2 (Seven)

Then open another terminal and run "aireplay-ng -0 5 –a 0A:86:20:5D:C9:95 –c F0:3D:03:62:93:57 wlan0mon". This command will deauthenticate the target client with the MAC address F0:3D:03:62:93:57 from the AP.

Figure 10: Steps to carryout Dictionary attack against WPA2 (Eight)

During the process of deauthenticating and reauthenticating the client, the 4-way handshake is captured by airodump-ng in the other terminal. This is shown in Figure 11 below.

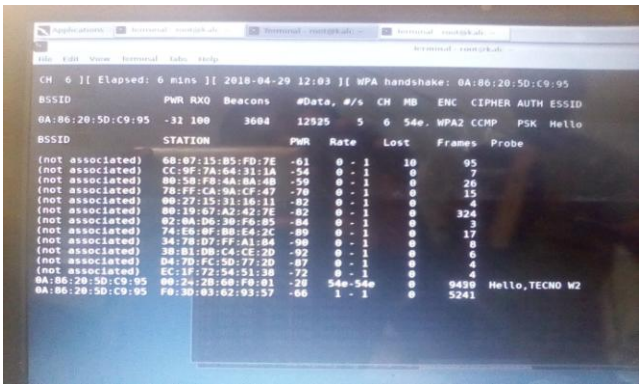
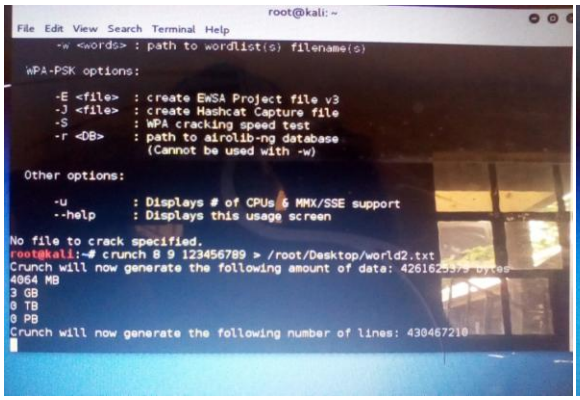


Figure 11: Steps to carryout Dictionary attack against WPA2 (Nine)

It should be noted that the captured handshake will be saved to the location we created that is /root/Desktop/capture. Then a wordlist was created using crunch. Wordlist is the dictionary that will be used for the attack. Hence, for the attack to be successful the dictionary must contain the passphrase for the targeted AP. Using crunch, we can create any dictionary such as figures, alphabets, alphanumeric, etc.
Then press Ctrl+C to stop the airodump-ng capturing terminal and create the wordlist.
To create the wordlist run "crunch 8 9 123456789> /root/Desktop/world2.txt." In the command above:
8 9 123456789 - means crunch should generate a passphrase that has a length of between 8 and 9 and that it should be made up of numbers i.e 123456789.



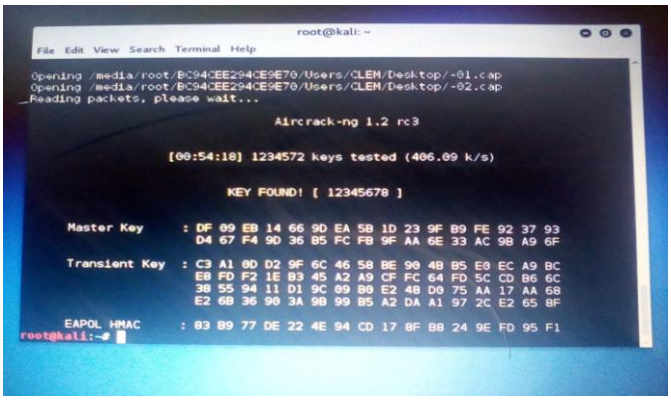


Fig. 12 Fig. 13

Figure 12: Steps to carryout Dictionary attack against WPA2 (Ten)

After the wordlist is created, then run "aircrack-ng –w root/Desktop/world2.txt root/Desktop/*.cap"

Figure 13: Steps to carryout Dictionary attack against WPA2 (Eleven)

From Figure 13, it was observed that aircrack-ng was able to recover the key in 54min 18 sec.

VI. COUNTERMEASURES

Our countermeasures are divided into two categories:

VI.1 The Body Implementing the Data Confidentiality Protocol

The body implementing the data confidentiality protocol should ensure that during the process of handshake, no key is installed twice. When a client receives retransmission of message 3 from the AP, it should only send an acknowledgement without reinstalling the session key. This will prevent key reinstallation attack.

Secondly, they should make sure that the nonce and replay counter are not reset when keys are reinstalled.

VI.2 Wireless Device Users

Wireless device users should ensure that they choose a lengthy key (passphrase) that is mixed with figures, alphabets and other special keys. Although, when the right dictionary is created no key cannot be recovered, it can take weeks or months before some keys can be recovered when they are lengthy and mixed with other special characters. The lengthier a key is, the longer time it will take to recover it. Also, wireless device users should check their Wi-Fi manufacturers' website for security patches and update them as soon as they are available.

VII. CONCLUSION AND RECOMMENDATIONS

For a long time, WPA2 has been providing the highest form of security for Wireless Local Area Network (WLAN). Unfortunately, it has been proven that even the highly placed WPA2 has some security flaws. The basic flaws are as a result ofthe reinstallation of keys during the handshake between AP and client which is a problem from the standard or protocol itself. In this paper, we were able to investigate and analyze in-depth of the process involved in the 4-way handshake which is dominantly used in WPA2. We also experimented how dictionary attack can be carried out against WPA2. Thus, we discovered that even the supposedly secured WPA2 is hack-able. Finally, for now, unless security patches are made available by the various AP vendors or a permanent solution against WPA2 attacks, WPA2 is not secured. Hence, we recommend that administrators should be all ears pending on when security patches will be released by AP vendors but before then, caution should be taken.

REFERENCES

[1] Choi, MK, Robles,R., Hong, CH and Kim, TH "Wireless Network Security: Vulnerabilities, Threats and Countermeasure", International Journal of Multimedia and Ubiquitous Engineering, Vol. 3, No. 3, (2008), Pg.. 77 – 86.

[2] Abiona, O., Oluwaranti, A., Oluwatope, A., Bello, S., Onime, C., Sanni, M and Kehinde, L. "Wireless Network Security: The Mobile Agent Approach", International Journal of Communications, Network and System Sciences, 6, (2013), Pg. 443 – 450

[3] Prodanovic, R and Simic, D. "A Survey of Wireless Security", Journal of Computing and

Information Technology – CIT, Vol 15, No 3, (2007), pp. 237 – 255

[4] Orukpe, P.E., Erhiaguna, T.O and Agbontaen, F.O. "Computer Security and Privacy in Wireless Local Area Network in Nigeria", International Journal of Engineering Research in Africa, Vol 9, (2013), Pg. 23 – 33

[5] Wikipedia, "Wired Equivalent Privacy,"https://en.m.wikipedia.org/wiki/wired_Equivalent_Privacy#Security-details

[6] Guillaume Lehembre, "Wi-Fi security – WEP, WPA and WPA2", www.hakin9.org

[7] Bilger, J., Cosand, H., Noor-E-Gagan Singh, NEG and Xaview, J. "Security and Legal Implications of Wireless Networks, Protocols and Devices

[8] Sithirasenan, E., Zafar, S and Muthukkumarasamy, V. "Formal Verification of the IEEE 802.11i WLAN Security Protocol", In Australian Software Engineering Conference (ASWEC 06), Pg. 181 – 190

[9] Vanhoef, M and Piessens, F. "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2", 2017.

[10] Eum, SH., Kim, YH and Choi, HK. "A Secure 4-Way Handshake in 802.11i Using Cookies", International Journal of Principles and Applications of Information Science and Technology, Vol 2, No 1, (2008).