WIRELESS NETWORKING: THREATS AND SECURITY

Dr. Sandeep Gupta
Assistant Prof., Department of Physics, Punjabi University College, Dhilwan, Barnala, Punjab
Dr. Sandeep Sharma
Assistant Prof., Department of Maths, Punjabi University College, Dhilwan, Barnala, Punjab

ABSTRACT-In the recent world advanced technology coupled with increasing price/ performance advantages, wireless accessibility is being deployed increasingly in office and public environments. Wireless local area network (WLAN) devices, for instance allow users to move their laptops from place to place within their offices. However threats are associated with recent technology. So it is the demand of the day to recognize threats and manage them. By this paper some security measures such as WEP, WPA, WPA 2 and usage of random numbers are discussed which include solutions for the sake of cyber security, so that security problems can be solved up to some extent.

***KEY WORDS*-Wireless local area network (WLAN),Wired equivalent privacy (WEP), Wi-fi protected access (WPA) and Wi-fi protected access II (WPA 2).**

INTRODUCTION

Wireless networking presents many advantages productivity and sensivity improves because of increased accessibility to information resources. Network configuration and reconfiguration is easier, faster, and less expensive. However, wireless technology also creates new threats and alters the existing information security risk profile. For example, dataInterception, denial of Service, Rogue Aps, wireless Intruders, misconfigured aps, endpoint attacks, wireless phishing and evil twin aps. [1].Also wireless networking alters the risks associated with various threats to security, the overall security objectives remain the same as with wired networks: preserving confidentiality, ensuring integrity, and maintaining availability of the information and information systems. The objective of this paper is to basic understanding of the nature of the various threats associated with wireless networking. The popularity of wireless Networks is a testament primarily to their convenience, cost efficiency, and ease of integration with other networks and network components. The majority of computers sold to consumers today come pre-equipped with all necessary wireless Networks technology. Over all we say “With every advance come new challenges”.

Although Wi-Fi network based on IEEE 802.11 standard are being widely deployed in different environment due to its standard. It allows an internet connection to be broadcast through radio waves. But the main problem of networking is interference of security and signal.

Through the last two decades wireless network researchers have come with 3 main Security protocols: WEP, WPA and WPA2. WEP was the first protocol introduced in the first IEEE 802.11 standard, received a great deal of coverage due to various technical failures in the protocol. WPA came with the purpose of solving the problems in the WEP cryptography method. WPA2 also known as IEEE 802.11i standard is an amendment to the 802.11 standard which specifying security mechanisms for wireless networks. The TCP/IP protocol suite, which is very widely used today, was developed under the sponsorship of the Department of Defense.

RELATED WORK

L.Jacob et al reviews the status of commercial and residential approaches to wireless network security and given justification for a project to assess the security status of wireless network usage in society and useful for providing input into a defence and attack methodology for improving the security of residential and commercial use of wireless networks**[2].**Li and Garuda **[3]**, DeagShiyang**[4]** discuss various encryption standards relating to 802.11 WLAN, their vulnerabilities and security flaws.Md. Waliullah et al discuss the various security issues and vulnerabilities related to the IEEE 802.11 wireless LAN encryption standard and common threats pertaining to the home and enterprises wireless LAN system and provide overall guidelines and recommendation to the home users and organization[5].S. vibhuti discusses about concepts and weaknesses of WEP protocol, also lists some of the available solutions for the WEP vulnerability**[6].** A. Rajalakshmiproposed that WEP and WPA both protocols are used to encrypt the current data and information, so that the un authorized and hackers cannot be able decrypt the data and hack the wireless fidelity networks. Many accessories can be linked with the wireless fidelity network with the help the access point (AP). The Wi-Fi signals provide an effect called interference. It has been considered on the channels known as ZigBee channels. In this paper, Packet Error Rate has been linked with the Wi-Fi Signals. Then the Packet Error Rate (PER) is connected with ZigBee channels and the calculations are done. Here Packet Error Rate gets raised when the Wi-Fi Channel comes closer.[7]. V.Wekhande discuss in paper that Wi-Fi products have a better scope in the Internet world. Wi-Fi network hold up roaming with various devices like cell phones, PC and also with portables accessories like laptops through Wi-Fi gaming is also possible. Wired Equivalent Privacy is used for the security reason and also it develops better verification, permission, encryption potentials gradually. Wi-Fi Protected Access can be formed with the assistance of the Wireless Fidelity Alliance. Here Wireless Access

Points (APs) provides very secured data for the transmission purpose. Commercial Wi-Fi can be used in enlarge places like college, companies, airports etc. Some kind of operation problems occurs when the connectivity speed is slow[8].

BRIEF HISTORY

First commercial WLAN systems with its Altair product developed by Motorola . However, earlyWLAN technologies had several problems that prohibited its pervasive use. These LANs were expensive,provided low data rates, were prone to radio interference, and were designed mostly to proprietary RFtechnologies. In 1990 IEEE initiated the 802.11 project with a scope “to develop a Medium AccessControl (MAC) and Physical Layer (PHY) specification for wireless connectivity for fixed, portable, andmoving stations within an area. In 1997, IEEE first approved the 802.11 international interoperabilitystandard. Then, in 1999, the IEEE ratified the 802.11a and the 802.11b wireless networkingcommunication standards. The mission was to create a standards-based technology that could span multiplephysical encoding types, frequencies, and applications. The 802.11a standard uses orthogonal frequencydivision multiplexing (OFDM) to reduce interference. This technology uses the 5 GHz frequencyspectrum and can process data at up to 54 Mbps. These numbers will vary immensely depending on the operating environment (obstacles and material construction) and theequipment used, for outdoorranges high gain directional antennas can exceed 20 miles.

WIRELESS NETWORK SECURITY

Although this section of the document focuses on the IEEE 802.11 WLAN standard, it is important tonote that several other WLAN technologies and standards are available from which consumers maychoose, including HiperLAN and HomeRF. For information on the European TelecommunicationsStandards Institute (ETSI) developed HiperLAN, visit the HiperLAN Alliance site.For moreinformation on HomeRF, visit the HomeRF Working Group site[9].

BENEFITS

WLANs offer four primary benefits:

Mobility of user: Users can access files, network resources, and the Internet without having tophysically connect to the network with wires. Users can be mobile yet retain high-speed, real-timeaccess to the enterprise LAN.

Rapid Installation: Network connections canbe made without moving or adding wires, or pulling them through walls or ceilings, or makingmodifications to the infrastructure cable plant so the time required for installation is reduced. For example, WLANs are often cited as making LANinstallations possible in buildings that are subject to historic preservation rules.

Flexibility: Enterprises can also enjoy the flexibility of installing and taking down WLANs inlocations as necessary. Users can quickly install a small WLAN for temporary needs such as aconference, trade show, or standards meeting.

Scalability: WLAN network topologies can easily be configured to meet specific application andinstallation needs and to scale from small peer-to-peer networks to very large enterprise networks thatenable roaming over a broad area[9].

GENERAL ATTACKS/THREATS TO WLAN

An attack is an action that is carried out by an intruder in order to compromise information in an organization. Unlike wired networks, a WLAN uses radio frequency or infrared transmission technology for communication; thus, making them susceptible to attack. These attacks are aimed at breaking the confidentiality and integrity of information and network availability. Attacks are classified into the following two categories: General Attacks/Threats to WLAN Technology

Passive attacks and Active attacks

Now a days, various attackers try to obtain the information that is being transmitted or received by the network, such attacks are called passive attacks. These types of attacks are usually very difficult to detect as there is no modification of the contents by the attacker [10]. There are two types of passive attack and these are traffic analysis and eaves dropping.

On the other hand, many times the information/contents are changed or fraudulent information may be even generated on the network also gains access to the information on the network, such attacks are known as passive attacks. This type of malicious act, results in great loss for any organization [10].

Following are a list of active attacks in WLAN technology:

Unauthorized Access,Rogue Access Point,Man in the Middle Attack (MITM),Denial-of-Service,Reply Attack,Session High jacking Furthermore, two other principals involved i.e. access control and authentication. Confidentiality is the prevention of intentional/unintentional disclosure of data. Integrity is control over the intentional/unintentional modification of data. Availability is the control over provision of system resources on demand to authorized users/systems/processes. Access control is the control of access to the resources by a legitimate user.Authentication is the process by which a system verifies the identity of a user who wants to access it [11].

THREE MAJOR GENERATIONS OF SECURITY APPROACHES

1. WEP(Wired Equivalent Privacy)
2. WPA(Wi-Fi Protected Access)
3. WPA2/802.11i(Wi-Fi Protected Access, Version 2)

There is a great possibility that Wireless threats come in all shapes and sizes, from someone attaching to your WAP (Wireless access point) without authorization, to grabbing packets out of the air and decoding them via a packet sniffer. This section discusses the most common threats faced by adding a wireless component to your network.

WLAN traffic travels over radio waves that the walls of a building cannot completely constrain. Although employees might enjoy working on their laptops from a grassy spot outside the building, intruders and would-be hackers can potentially access the network from the parking lot or across the street using the Pringles can antenna.

Wireless networks are susceptible and exposed to attack because of its borderless nature. It is easy to penetrate any wired network via wireless network as Access Point (AP) is bridging between wireless and wired network. Packet sniffing can be done passively because of the hub-based configuration of the APs. Moreover, hacking tools are largely available in the market and online. These tool which are usually meant to be used by penetration testers and for educational purposes are being misused and abused by underground or even novice hackers. On the other hand, the flexibility of mobile devices such as smart phones, tablets and laptops are the main reason of the popularity of hotspots which are exposed of the rogue access points. Another feature of newly developed smart phones which is tethering introduces more security issues to the end users. Also wireless IPS products like Motorola air defence, air magnet and air tight can also detect malicious Wi-Fi clients operating in or near a business' airspace by wireless intruders.

Specific threats and vulnerabilities to wireless networks and handheld devices include the following:

All the vulnerabilities that exist in a conventional wired network apply to wireless technologies.Malicious entities may gain unauthorized access to an agency's computer network through wirelessconnections, bypassing any firewall protections.Sensitive information that is not encrypted (or that is encrypted with poor cryptographic techniques)and that is transmitted between two wireless devices may be intercepted and disclosed.DoS attacks may be directed at wireless connections or devices.Malicious entities may steal the identity of legitimate users and masquerade as them on internal orexternal corporate networks.Sensitive data may be corrupted during improper synchronization. Malicious entities may be able to violate the privacy of legitimate users and be able to track theirmovements. Malicious entities may deploy unauthorized equipment (e.g., client devices and access points) tosurreptitiously gain access to sensitive information.Handheld devices are easily stolen and can reveal sensitive information.Data may be extracted without detection from improperly configured devices.

WIRELESS NETWORK SECURITY

On a wireless device data may be corrupted by Viruses or other malicious code and subsequently beintroduced to a wired network connection.Through wireless connections,malicious entities may connect to other agencies or organizations forthe purposes of launching attacks and concealing their activities.Interlopers, from inside or out, may be able to gain connectivity to network management controls andthereby disable or disrupt operations.Third-party, untrusted wireless network services may be used by malicious entities, the purpose behind it is to gain access to anagency's or other organization's network resources.Internal attacks may be possible via ad hoc transmissions.This document provides an overview of wireless networking technologies and wireless handheld deviceswhich are most commonly used in an office environment and with today's mobile workforce. It also seeksto assist agencies in reducing the risks associated with 802.11 wireless local area networks (LAN),Bluetooth wireless networks, and handheld devices.

Significant effort, resources, andvigilance are required for maintaining a secure wireless network and associated devices and involve the following steps:

- Labelling and keeping inventories of the fielded wireless and handheld devices.
- Creating backups of data frequently
- Maintaining a full understanding of the topology of the wireless network
- Performing periodic security testing and assessment of the wireless network
- Performing on-going, randomly timed security audits to monitor and track wireless and handhelddevicesApplying patches and security enhancements
- Vigilantly monitoring wireless technology for new threats and vulnerabilities
- Monitoring the wireless industry for changes to standards that enhance security features and for the release of new products

WEP(WIRED EQUIVALENT PRIVACY)

WEP protocol defines a set of instructions and rules by which wireless data can be transmitted over the airwaves with some amount of security.WEP Algorithm and its vulnerabilities was an encryption algorithm designed toprovide wireless security for users implementing 802.11 wireless networks. The intention was to offersecurity through an 802.11 wireless network while the wireless data was transmitted from one end point to another over radio waves. WEP was used toprotect wireless communication from eavesdropping (confidentiality), preventunauthorized access to a wireless network (access control) and preventtampering with transmitted messages (data integrity).WEP uses the RC4 stream cipher, combining a 40-bit WEP key with a 24-bitrandom number known as an Initialization Vector (IV) to encrypt the data.

Weaknesses of WEP are tomaintaining a shared WEP key it has disabled a high percentage of wireless networks.WEP has the same problem as the shared key secret is held by another person the private key it becomes public key.The WEP checksum is linear and predictable. On the other hand Strengthening of WEP are Instead of using CRC checksum, different method can be used for the data integrityverification like hash functions.Change secret key regularly, dynamically using secure symmetric key distributionprotocols.Better key management using security handshake protocols and new authentication mechanisms using the Extensible Authentication Protocol (EAP).

Generally WEP was considered as a broken protocol.The vulnerability of WEP can be attributed to the following:

- WEP key recovery
- Unauthorized decryption and the violation of data integrity
- Poor key management and No access point authentication

SOLUTIONS TO WEP

Various vendors led the ways to produce their own solutions to address the weakness in WEP.

Enhanced WEP key: In 1998, Lucent pioneered a 128-bit WEP to extend the WEP key from 40-bit to 104-bit in order to enhance security. Under this approach, attackers might take longer amount of time to break the enhanced WEP keys. However, the approach was not very helpfulbecause the previous security flaws in WEP still persisted.

Dynamic WEP key: Later, several vendors, including Cisco and Microsoft, implemented dynamic WEP re-keying of access points. Theidea was to automatically generate short-lived, dynamic broadcast WEPkeys at an interval set by a system administrator. The dynamic WEP keys prevented attackers from eavesdropping the communications. The attackers might never collect enough data to crack WEP keys.

The implementation of VPNs: The wireless network can be further protected with the implementation of VPNs. Although VPN hardware may enable remote devices to establish a secure connection to access points, the VPN solution may fail to address seamless roaming when access points are cross, overall the specific solutions from vendors may lead to poor interoperability in the long run.

Solutions available to overcome the weaknesses of WEP

- The size of the Initialization Vector (IV) should be bigger while choosing.
- The hashed value of IV can be prepended or appended to the ciphertext instead of theclear text.
- Change secret key regularly, dynamically using secure symmetric key distributionprotocols.
- Better key management using security handshake protocols.
- New authentication mechanisms using the Extensible Authentication Protocol(EAP).

Wi-Fi PROTECTED ACCESS (WPA)

Due to the limitations of WEP, the WPA came into existence.WPA is the subset of theIEEE’s 802.11i wireless security specification.Temporal Key Integrity protocol (TKIP) is the encryption method of WPA. The weaknesses ofWEP addresses by TKIP by including mixing function, a message integrity check, an extendedinitialization vector, and a re-keying mechanism. The compatible version of IEEE 802.11i is WPA, which is under development. To implementWPA both server and client computers updates their software’s during 2003.WEP/WPA modes access points can operate to support both WEP and WPA clients. WEP security level iscompatible with mixed level security for all users. The Wi-Fi Protected Access (WPA) is a standards-based interoperable security specification. The specification is designed so that only software or firmware upgrades are necessary for the existing or legacy hardware to meet the requirements. Its purpose is to increase the level of security for existing and future wireless LANs.

SOLUTIONS TO WPA

Use an inconspicuous network name (SSID)

The service set identifier (SSID) is one of the most basic Wi-Fi network settings. Though it doesn’t seem like the network name could compromise security, it certainly can. Using a too common of a SSID, like “wireless” or the vendor’s default name, can make it easier for someone to crack the personal mode of WPA or WPA2 security. This is because the encryption algorithm incorporates the SSID, and password cracking dictionaries used by hackers are preloaded with common and default SSIDs. Using one of those just makes the hacker’s job easier.Although it might make sense to name the SSID something easily identifiable, like the company name, address, or suite number, that might not be the best idea either. This is especially true if the network is in a shared building or in close proximity to other buildings or networks. If hackers drive by a congested area and see a dozen different Wi-Fi networks pop-up, they would likely target the one easiest to identify, which could help them understand what they might gain by hacking it. They might also choose one that’s easier to find in a congested area.

It is possible to turn off SSID broadcast, essentially making the name of your network invisible, but I don’t suggest that. Forcing users to manually enter the SSID, and the negative performance effects of probe requests on the Wi-Fi, typically outweigh the security benefit. And someone with the right tools can still capture the SSID from sniffing other network traffic.

Remember physical security

Another physical security concern with Wi-Fi is when someone adds an unauthorized AP to the network, typically called a “rogue AP.” This could be done for legit reasons by an employee wanting to add more Wi-Fi coverage or for ill-intended purposes by an employee or even an outsider who gains access to the facility. To help prevent these types of rogue APs, ensure any unused ethernet ports (like wall ports or loose ethernet runs) are disabled. You could physically remove the ports or cables, or disable the connectivity of that outlet or cable on the router or switch. Or if you really want to beef up security, enable 802.1X authentication on the wired side, if your router or switch supports that, so any device plugging into the ethernet ports has to enter log-in credentials to gain network access.

Wireless security or all of IT security for that matter isn’t all about fancy technologies and protocols. You can have the best encryption possible and still be vulnerable. Physical security is one of those vulnerabilities. Locking down just your wiring closets isn’t enough, either.

Most access points (APs) have a reset button that someone can press to restore factory default settings, removing the Wi-Fi security and allowing anyone to connect. Thus, the APs distributed throughout your facility need to be physically secured as well to prevent tampering. Ensure they are always mounted out of reach and consider using any locking mechanisms offered by the AP vendor to physically limit access to the AP buttons and ports.

Security Features of 802.11 Wireless LANs per the Standard:

The three basic security services defined by IEEE for the WLAN environment are as follows:

Authentication: A primary goal of WEP was to provide a security service to verify the identity ofcommunicating client stations. This provides access control to the network by denying access to client stations that cannot authenticate properly. This service addresses the question, “Are only authorizedpersons allowed to gain access to my network?”

Confidentiality: Confidentiality, or privacy, was a second goal of WEP. It was developed to provide“privacy achieved by a wired network.” The intent was to prevent information compromise fromcasual eavesdropping (passive attack). This service, in general, addresses the question, “Are onlyauthorized persons allowed to view my data?”

Integrity: Another goal of WEP was a security service developed to ensure that messages are notmodified in transit between the wireless clients and the access point in an active attack. This serviceaddresses the question, “Is the data coming into or exiting the network trustworthy—has it beentampered with?”

WPA2/802.11i(Wi-Fi PROTECTED ACCESS VERSION 2)

IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands.

The 802.11i specification is a solution that IEEE 802.11 committee designs totarget the security problems created by the WEP. The 802.11 Task Group “I” hasbeen spending more than two years on the specification and three drafts havebeen released ever since. The specification includes several key features:

Encryption algorithms TKIP - In order to support legacy device, the 802.11i chooses TKIPas one of the encryption standard (same as WPA). CCMP – 802.11i also includes another standard known as AESCCMP.AES stands for advanced encryption standard, which is amuch stronger encryption algorithm that the US National Institutesof Standards and Technology (NIST) chose AES to replace theaging Data Encryption Standard (DES). However, AES-CCMPrequires a hardware coprocessor to operate. Therefore, extrahardware is needed in the implementation of AES-CCMP. Also other benefits are Stronger Encryption through the implementation of AES and Roaming Support given by it. But for implementation of AES-CCMP An extra requirement in hardware upgrade is required.

Also TCP/IP protocol suite as random number process, which is very widely used today, was developedunder the sponsorship of the Department of Defense. Despite that, there are anumber of serious security flaws inherent in the protocols, regardless of thecorrectness of any implementations. There are variety of attacks based onthese flaws, including sequence number spoofing, routing attacks, sourceaddress

spoofing, and authentication attacks.

SOLUTIONS TO WPA

Use Enterprise WPA2 with 802.1X authentication

Deploying the enterprise mode Wi-Fi security is one of the most beneficial Wi-Fi security mechanisms you can put into place, because it authenticates every user individually: Everyone can have their own Wi-Fi username and password. So if a laptop or mobile device is lost or stolen, or an employee leaves the company, all you have to do is change or revoke that particular user’s log-ins.

In personal mode, by contrast, all users share the same Wi-FI password, so when devices go missing or employees leave you have to change the password on every single device a huge hassle.

Another great advantage of enterprise mode is that every user is assigned his or her own encryption key. That means users can only decrypt data traffic for their own connection no snooping on anyone else’s wireless traffic.

To put your APs into enterprise mode you'll first need to set up a RADIUS server. This enables user authentication and connects to or contains the database or directory (such as Active Directory) that holds everyone’s usernames and passwords.

Although you could deploy a standalone RADIUS server, you should first check if your other servers (like a Windows Server) already provide this function. If not, consider a cloud-based or hosted RADIUS service. Also keep in mind that some wireless access points or controllers provide a basic built-in RADIUS server, but their performance limits and limited functionality typically make them only useful for smaller networks.

Secure the 802.1X client settings

Like other security technologies, the enterprise mode of Wi-Fi security still has some vulnerabilities. One of these is man-in-the-middle attacks, with a hacker sitting in an airport or cafe, or even outside in the parking lot of a corporate office, by which a fake Wi-Fi network with the same or similar SSID could be set up as the network they’re trying to imitate; when your laptop or device attempts to connect, a bogus RADIUS server could capture your login credentials. The thief could then utilize your login credentials to connect to the real Wi-Fi network.

A way to prevent man-in-the-middle attacks with 802.1X authentication is to utilize server verification on the client side. When server verification is enabled on the wireless client, the client won’t pass your Wi-Fi login credentials to the RADIUS server until it verifies it’s communicating with a legit server. The exact server verification capabilities and requirements you can impose on the clients will vary, depending upon the device.

In Windows, for instance, you can enter the domain name(s) of the legit server, select the certificate authority that issued the server’s certificate, and then choose to not allow any new servers or certificate authorities. So if someone has set up up a fake Wi-Fi network and RADIUS server and you try to log on to it, Windows will stop you from connecting.

Use rogue-AP detection or wireless intrusion prevention

We’ve already touched on three vulnerable access point scenarios: One where an attacker could set up a fake Wi-Fi network and RADIUS server, another where someone could reset an AP to factory defaults, and a third scenario where someone could plug in their own AP.

Each of these unauthorized APs could go undetected by IT staff for a long period of time if proper protection isn't put in place. Thus, it's a good idea to enable any type of rogue detection offered by your AP or wireless controller vendor. The exact detection method and functionality vary, but most will at least periodically scan the airwaves and send you an alert if a new AP is detected within range of the authorized APs.

For even more detection capabilities, some AP vendors offer a full-fledged wireless intrusion detection system (WIDS) or intrusion protection system (WIPS) that can sense a range of wireless attacks and suspicious activity along with rogue APs. These include erroneous de-authentication requests, mis-association requests, and MAC address spoofing.

Furthermore, if it's a true WIPS offering *protection* rather than a WIDS offering just *detection*, it should be able to take automatic countermeasures, such as disassociating or blocking a suspect wireless client to protect the network under attack.

If your AP vendor doesn't provide built-in rogue AP detection or WIPS capabilities, consider a third-party solution. You might look at sensor-based solutions that can monitor both Wi-Fi performance and security issues, from companies like 7SIGNAL, Cape Networks and Net Beez.

Join the Network World communities on Facebook and LinkedIn to comment on topics that are top of mind.

CONCLUSION

In the world of advance technology, where wireless networking provides numerous opportunities to increase productivity and cut costs, it also alters an organization's overall computer security risk profile. Although totalelimination of all risks associated with wireless networking is impossible, but to achieve a reasonable level of overall security by adopting a systematic approach to assessing and managing risk is quite possible. This paper discussed the threats and vulnerabilities associated with each of the three basic technology components of wireless networks (clients, access points, and the transmission medium) and described various commonly available countermeasures that could be used to mitigate those risks. It also stressed the importance of training and educating users in safe wireless networking procedures.

REFRENCES

1. M.K.Choi, R.J.Robles, C.Hong and T. Kim," Wireless Network Security: Vulnerabilities, Threat and Countermeasure" International journal of Multimedia and Ubiquitous Engineering Vol.3, pp. 77-86, July 2008.
2. L.Jacob, D. hutchinson and J. Abawajy," Wi-Fi Security : wireless with confidence, Proceedings of the 4th Australian Security and Intelligence Conference,Citigate Hotel, Perth, Western Australia,5 – 7 December, 2011.
3. J.Li.M.Garuba," Encryption as an effective tool in reducing wireless LAN Vulnerabilities," Fifth International Conference on Information Technology, New Generations, Las Vegas, Nevada, 7-9 April 2008, pp. 557-562.
4. D.Shiyang," Compare of new security strategy with several others in WLAN," IEEE 2nd International Conferences on computer Engineering and Technology, Chengdu, China, 16-18 April, 2010. Pp. 24-28.
5. Md. Waliullah and D. Gan," Wireless LAN security threats and Vulnerabilities," International journal of advanced computer science and applications (IJACSA), Vol. 5, No. 1, 2014.
6. S. vibhuti ,"IEEE 802.11 WEP (Wired Equivalent Privacy) Concepts and Vulnerability," CS 265 Spring 2005.
7. A. Rajalakshmi and G. Kapilya," The Enhancement of Wireless Fidelity (Wi-Fi) Technology, Its Security and Protection Issues," ISSN 2319-5991, Int.J.Engg.Res& Sci. &Tech. 2014, pp. 179-183.
8. VandanaWekhande (2006), "Wi-Fi Technology: Security Issues", Rivier Academic Journal, Vol. 2, No. 2.
9. Tom T. Karygiannis, L Owens," Wireless Network Security: 802.11, Bluetooth and Handheld Devices," November 01, 2002,NIST Pub Series: Special Publication (NIST SP) - 800-48.
10. B. Forouzan, Data Communications & Networking. 4th edition. New York: McGraw-Hill, 2008.
11. Search Security, (2011) Information security tutorials [Online], Available at: http://searchsecurity.techtarget.com/tutorial/Information-security-tutorials, [Accessed on: 14/11/12].