Recurrent Security Gaps In 802.11ac Routers

Mohammed Farik, ABM Shawkat Ali

Abstract: In comparison to earlier IEEE 802.11 standard (a/b/g/n) routers, today's popular 802.11ac standard routers have enhanced security. However, 802.11ac router still has major security vulnerabilities. The novelty of this paper is that we not only highlight multiple security vulnerabilities in 802.11ac router technologies that still have not been secured since the earlier standards, but also present some new ideas with solutions. We believe that our line of thoughts on security vulnerabilities, gaps, and on new solutions will provide network security researchers, router manufacturers and network administrators with new disclosures to redesign even better security mechanisms in routers to counter attacks on networks via routers.

Index Terms: backdoor ports, gaps, IEEE 802.11ac, password, vulnerability, wireless routers, WPA2

1 INTRODUCTION

ALL wireless network devices have to be compatible to one another in order to communicate. This compatibility is maintained through standards. The Institute of Electrical and Electronics Engineers (IEEE) has developed a few prominent wireless network standards and amendment since the initial 802.11 standard in 1997, namely 802.11a, 802.11b, 802.11g, security amendment 802.11i, 802.11n and the 802.11ac [1]. Each standard implemented a few improved characteristics, such as better security using 802.11i standard. A router is a network device that connects networks having the same or different access methods and media, such as Ethernet to token rings. It forwards packets to networks by using a decision-making process based on the routing table data, discovery of the most efficient routes, and preprogrammed information from the network administrator [2]. On the other hand, an access point (AP) is a device that attaches to a cabled network and that services wireless communication between wireless network interface cards (WNICs) and the cabled network. An access point can also act as a central point of communications for all wireless networks [2],[3]. In this paper, we are using the term wireless router as functions of router and access point are today combined in a single device – the wireless router. Today, 802.11ac standard is available in wireless routers that are being sold by major router vendors in Fiji and these routers are being widely deployed in wireless local area network (wireless LAN or WLAN) in homes and office environments. The 802.11ac routers (also known as 5G Wi-Fi) offers a maximum of 1733 Mbps of wireless connection speed on the 5GHz frequency band, are backwards compatible with prior standards (a/b/g/n), and thus support all existing Wi-Fi clients on the wireless network [4]. Much of its success is due to the easy installation feature, greater speeds, and connectivity to home entertainment systems. Wireless routers with 802.11ac standard offers a whole range of improved features [5]. Features such as USB 3.0 interface enable new WLAN scenarios like HD video streaming to multiple clients in home, backup of large data files, wireless display, FTP servers, personal cloud services and more. However, the problem is that despite the many enhancements down the line in standards and wireless router technologies, there are still some persistent security vulnerabilities or gaps in 802.11ac routers. Attackers can capitalize on these loopholes in 802.11ac routers to attack wireless networks thus requiring better solutions. These routers have to be secured to prevent next-door neighbors or intruders connecting to a wireless network via its weaknesses (Fig.1). The novelty of this paper is that it presents a complete overview of security vulnerabilities or gaps that need to be patched up in 802.11ac routers in the future. As 802.11ac standard routers are installed in infrastructure mode wireless networks in homes and organizations, this paper first describes IEEE 802.11ac routers in infrastructure-mode WLAN architecture in section 2. Second, the paper discusses available wireless security mechanisms in IEEE 802.11ac WLAN routers, specifically security types, authentication and encryption in section 3. Third, currently unresolved vulnerabilities or security gaps in 802.11ac APs are discussed in section 4. Lastly, we suggest new recommendations in section 5, and summarize our findings at conclusions in section 6.

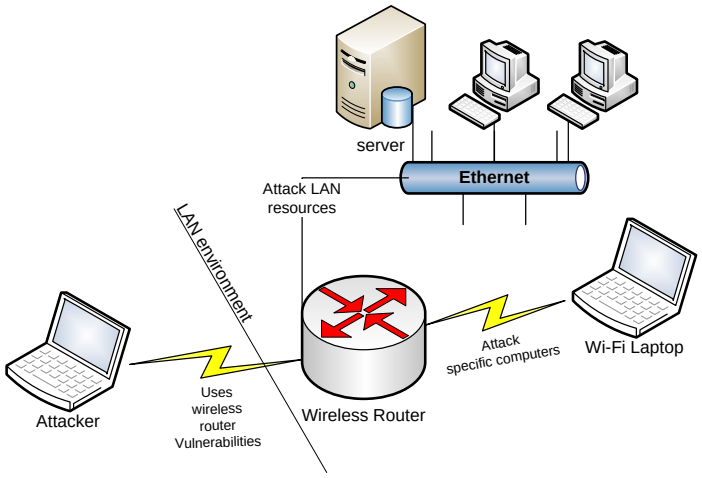

Fig.1. *Attack via Wireless Router*

2 WIRELESS ROUTER IN INFRASTRUCTURE NETWORK

Wireless or Wi-Fi technology uses radio frequency to connect wirelessly, providing the freedom to connect computers anywhere in home or office network. It does so strictly adhering to the IEEE 802.11 standards. A common type of wireless network is Wireless Local Area Network (WLAN) in Infrastructure mode, also known as basic service set mode (Fig.1). Infrastructure mode uses a wireless router as a base station to route transmissions between the sending and

- *Mohammed Farik is an Assistant Lecturer in Information Technology in the School of Science and Technology at The University of Fiji, PH-679-6640600. E-mail: mohammedf@unifiji.ac.fj*
- *ABM Shawkat Ali is a Professor in Information Technology in the School of Science and Technology at The University of Fiji.*

receiving devices on the wireless network [3]. Benefits of this setup include greater user mobility, greater flexibility, scalability in network setup, and also it is quicker to set up network. All the wireless devices or clients in a WLAN in Infrastructure mode will connect to the wireless router. A wireless router is a communication hardware that provides a single connection point for wireless connectivity in a network. It uses transmit/receive antennas for wireless connection and uses WAN/LAN ports for *Ethernet* or wired connection. The wireless router is hard-wired to the Ethernet (wired LAN) and it provides the communication link between the wireless client devices and any of the wired network devices (Fig.1). Components of a wireless router include an antenna and RF transmitter, communication software, and a wired network card, while a client PC will need a wireless network interface card (WNIC). However, today all recent laptop models come with a WNIC chip enabled on the mainboard. The features of a common 802.11ac wireless router are summarized in Table 1. Service Set Identifier (SSID) is the name of the wireless router, is 3 to 32 characters in length, and is case-sensitive. An access point sends out beacon messages to announce their presence and operating parameters to clients such as laptops. The service set identifier (SSID) is part of this beacon message that declares the wireless router's identity to wireless devices such as laptops. The message also contains signal strength (e.g. Strong), radio type (e.g. 802.11ac) and security type (e.g. WPA2-PSK). Some default values for SSID are *Default SSID, Wireless*, *WLAN* and brand name of router. Security concerns begin when the default values are not changed. A client looking for a specific network to join would scan for this SSID and when the network is discovered, the association process begins. The EC-Council states that the biggest disadvantage of a wireless router is its mobility [3]. We disagree that mobility is a problem. Mobility is the main reason why wireless routers were developed. We believe, instead weaknesses or holes in wireless router's security mechanisms are the biggest problem. A container may spill water while it is mobile, but if the container has holes, it will absolutely leak water even if it not moving.

TABLE 1

SUMMARY OF COMMON 802.11ac/n/g/b/a ROUTER

Features	
Dual Wireless Speed	2.4 GHz →600 Mbps 5GHz→ up to 1700Mbps
Wired Speed	10/100/1000Mbps ports
Modulation	OFDM
USB ports	2.0 3.0
WAN (Internet) Port	1
LAN (Ethernet) Ports	4
Buttons	Power on/off Wi-Fi on/off WPS/Reset
Antennas	2
Installation	Easy
Security/ Encryption	WEP WPA/WPA2 (Enterprise) WPA-PSK/WPA2-PSK (Personal) MAC Address Filtering Access Control
Firewall	SPI NAT

3 WIRELESS SECURITY IN ROUTERS

This section explains the different levels (types or modes) of security available in wireless routers. The different types are WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA-PSK (Pre-Shared Key), WPA2 (Wi-Fi Protected Access 2), and WPA2-PSK (Pre-Shared Key). WEP is the original wireless encryption standard. To use it, the user must enter the same key(s) into the router and the wireless stations. For 64 bit keys the user must enter 10 hex digits into each key box. For 128 bit keys, the user must enter 26 hex digits into each key box (Fig.2). A hex digit is either a number from 0 to 9 or a letter from A to F. for the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled. The user can also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64-bit keys, and a maximum of 13 characters for 128-bit keys. If the user chooses the WEP security option, the router will only operate in legacy wireless modes (802.11b/g). This means the user will not get 11n/ac performance due to the fact that WEP is not supported by Draft 11n/ac specification. WPA provides a higher level of security. WPA-Personal does not require an authentication server (Fig.3). WPA or WPA2 mode can be used to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security for stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, *WPA2 Only* mode should be used. This mode uses *AES(CCMP)* cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, *WPA Only* should be used. This mode uses *TKIP* cipher. Some gaming and legacy devices work only in this mode. To achieve better wireless performance *WPA2 Only* security mode (or in other words AES encryption cipher) should be used.

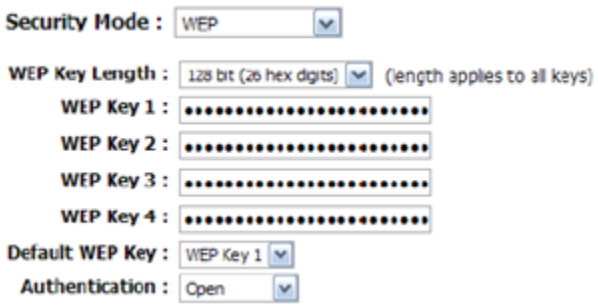

Fig. 2. *WEP Security in Router*

Additionally, a pre-shared key which is an 8 to 63 character alphanumeric passphrase should be entered. For good security it should be of ample length and should not be a commonly known phrase.

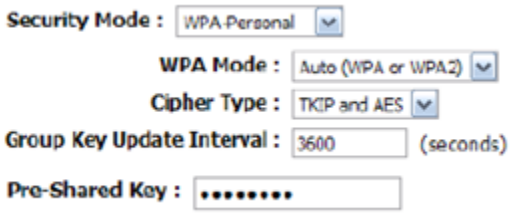

Fig. 3. *WPA/WPA2-Personal Security in Router*

The WPA-Enterprise option requires an external RADIUS server (Fig.4). When WPA enterprise is enabled, the router uses EAP (802.1x) to automate clients via a remote RADIUS server.

Fig. 4. *WPA/WPA2-Enterprise Security in Router*

4 VULNERABILITIES OR GAPS

Innovations in 802.11 wireless networks have been driven by efforts to eliminate security vulnerabilities or gaps in the existing wireless technologies. However, despite the many improvements, there are still many security gaps to be filled (Fig.5) which allows an attacker to hack into wireless network (Fig.1). Wireless networks are hacked via the wireless router in the following attack steps. First, the attacker finds network to attack. Second, the attacker chooses a network to attack. Third, the attacker analyses the network. Then the attacker cracks the passphrase, password, and/or encryption. Finally, the attacker sniffs the network [3]. Unsolved vulnerabilities present in today's 802.11ac wireless routers are in areas of SSIDs, default administrative passwords, MAC address, WEP, WPA/WPA2, and backdoor ports.

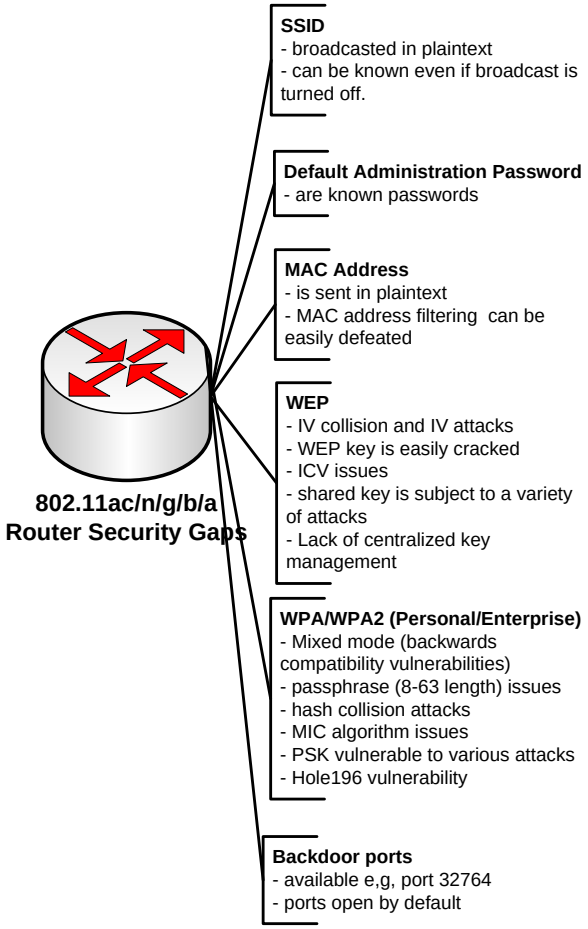

Fig. 5. *Security Gaps in Wireless Router*

Let's begin with default *SSID and beacon broadcast* vulnerabilities. A wireless router typically broadcasts the SSID so that nearby clients can connect to it. *Broadcast SSID* is normally enabled by default. If this feature is disabled, then an SSID must be configured manually in the client to match the SSID of the wireless router. If the default or manufacturer set SSID is not changed, an attacker may know from the SSID the model or make of the router being used. However, do not change the SSID to reflect a name, or location as it might attract attackers. However, SSID contained in the beacon frame is always sent in plaintext. Also, any wireless client can obtain the SSID even if SSID broadcast is turned off, because SSID will still be sent out in other management traffic, which can be sniffed by an attacker using tools such as *AiroPeek NX, Wireshark, vxSniffer, EtherPEG, AirMagnet, Driftnet, winDump, THC-RUT,* and *Microsoft Network Monitor* [3],[6]. Next is *default administration password*. Many routers, out of the manufacturer's box have a default password configured on the administrator account. If the password is not changed with a strong password, attackers can have an easy guess [6]. Next is *MAC address* vulnerability. Many wireless networking devices sends MAC address in cleartext even if WEP is enabled. Software tools like Airsnort identify the manufacturers based on the MAC address, so if only the SSID is changed, chances are that an informed attacker can easily gain access [6]. Also, software tools such as Ethereal can be used by an attacker to passively sniff the wireless traffic to find MAC addresses that are allowed on the network by the MAC

address filter. If MAC address filtering is the only security measure in place, attackers only need to change their own MAC address to one that is allowed [6],[7]. Moreover, a wireless router is normally configured with the most secure transmission encryption method compatible with the clients in the network. The choices include WEP, WPA/WPA2-Personal, WPA/WPA2-Enterprise. *WEP encryption* also has a number of unsolved vulnerabilities. First, WEP uses 64-bit or 128-bit number to encrypt packets made up of 24-bit IV and either a 40-bit or 104-bit default key. The length of IV remains 24-bits even if longer 128-bit number is used which means there will only be 16,777,216 possible values [7],[8]. If different IVs were used for each packet, then all IVs would be used up and start repeating in less than a few hours. Because of the weaknesses of WEP, it is possible for an attacker to identify two packets derived from the same IV (called a IV collision). With that information the attacker can begin what is called a keystream attack or IV attacks [3],[9]. Today, WEP key can be cracked in minutes using techniques such as automated tools, pad collection attacks, XOR encryption, and stream ciphers. Automated WEP cracking tools such as AiroPeek, Aircrack, AirPcap, WEPCrack, Airsnort, Network Stumbler, iStumbler, KisMAC, Kismet, and Cain & Abel [3] can be easily downloaded from the internet for attacking WEP programmed router. Second, *integrity check value (ICV),* which is input to the RC4 algorithm, is a checksum output from CRC-32 integrity algorithm and is not encrypted. ICV is used to ensure integrity of packets during transmission. It is possible for an attacker to forge cipher text without changing the checksum appended to the message and to inject messages without detection [7],[8]. There is no packet forgery protection in WEP. Even without knowing the encryption key, an adversary can change 802.11 packets in random, undetectable ways, deliver data to unauthorized parties, and masquerade as an authorized user [8]. Third is *Shared Key authentication.* During the challenge-response sequence, both the plaintext challenge and the encrypted challenge are transmitted. The key and the IV pair used for the authentication sequence can be discovered before the association is made and hence is vulnerable to attacks [7],[10]. Shared key used by WEP can be cracked using tools such as *Airsnort*, *WEPCrack*, and *Dweputils* within few minutes of data capture and analysis [8]. Also, the distributed shared key is the weakest aspect of the system. By using static shared keys, distributed among all the clients as password, the number of users aware of these keys will grow as the network expands [7] and hence will also increase vulnerability of attacks. Moreover, most manufacturers have configured their APs to use the same shared key, or the default four keys which makes it easy to determine the number of plaintext messages encrypted with the same key. The challenge-response scheme used in shared key authentication can lead to man-in-the-middle attack. Man-in-the-middle attacks set up illegitimate access points within range of wireless clients in order to gain access to sensitive information [8]. Moreover, associate and disassociate messages are not authenticated and this can lead to WEP be vulnerable to denial-of-service attacks. Fourth, *lack of centralized key management* makes it difficult to change WEP keys with any regularity. There is also no defined method for encryption key distribution so shared keys that are initially set during installation by administrator are rarely (if ever) changed [8]. The standard specified for WEP provides support for 40 bit key only, thus it is prone to brute force attacks. *WPA* was developed to improve on the weaknesses of WEP, and it did, but to some extent only. Vulnerabilities still exist because of various reasons. To start with, while WPA enhanced security, hackers also developed new methods on software tools such as *Reaver* and *Aircrack-ng* to crack WPA encryption [10],[11],[12]. However, cracking WPA takes a longer time than WEP. Next, wireless routers are still programmed with provisions for backward compatibility with earlier standards such as 802.11a/b/g, which means earlier unsafe security still remain in the new 802.11ac routers Hence the vulnerabilities can easily resurface in 802.11ac wireless network environment if mixed mode is configured in the router. Also, improper management of PSK keys can expose a WLAN to attackers. Here, like WEP the distribution and sharing of PSK keys is performed manually without any technology security protections. The keys can be distributed by insecure methods like telephone, email, or text message. Any user who obtains the key is assumed to be authentic and approved. Additionally, standard security practices call for keys to be changed on a regular basis. Changing the PSK key requires reconfiguring the key on every wireless device and on all access points. Moreover, to allow a guest user to have access to PSK WLAN, the key must be given to that guest. Once the guest departs, this shared secret must be changed on all devices to ensure adequate security for PSK WLAN [7]. A second area of PSK vulnerability is the use of passphrases. A PSK is a 64-bit hexadecimal number. The most common way this passphrase is generated is by entering a passphrase (consisting of letters, digits, punctuations, and so on) that is between 8 to 63 characters in length. PSK passphrases of fewer than 20 characters can be subject to dictionary attacks to crack the passphrase [7]. If a user created a PSK passphrase of fewer than 20 characters that was a dictionary word, then a match may be found and the passphrase broken. Moreover, WPA technology brought about a few new vulnerabilities of its own which are discussed here. First, WPA is prone to threats during hash collisions due to use of hash functions for TKIP key mixing [8]. Second, the Michael MIC algorithm in WPA provides a balance between data integrity, security and reduced processing requirements. Although it is an improvement over the original CRC32 [7] used in WEP, the Michael algorithm [7] is invertible and its key discoverable and therefore vulnerable to spoofing attacks. To address this vulnerability, designers of the WPA standard implemented a spoofing countermeasure, which terminates the wireless connection for one minute if more than two bad MICs are received in any one minute period. Unfortunately, this countermeasure is in itself a vulnerability because it may be used as a doorway to Denial-of-Service attacks [13] (by deliberately injecting packets with bad MICs), and in noisy RF environments, where packet errors are common, this countermeasure can inadvertently trigger and negatively affect the robustness of the wireless network [7],[13]. Third, although 802.1X authentication support was made mandatory in WPA, its use requires an external authentication server and so the user is given an option to use a simple pre-shared key (PSK) mechanism like WEP. Unfortunately, as with WEP, the PSK authentication mechanism in WPA is vulnerable to key management issues [14]. It is virtually impossible to keep a single shared key secret among a large community, and re-keying and distributing new keys for a large community is likewise difficult. The PSK is combined with other session-specific information exchanged during the 4-Way Handshake,

to generate a Pair-wise Transient Key (PTK), which is in turn used to generate dynamic encryption and message integrity keys [7],[14]. Although the short key and IV re-use issue has been resolved by this mechanism, a PSK is still vulnerable to dictionary attacks [10]. By capturing the 4-Way Handshake authentication exchange and using this information along with a dictionary file it is possible to successfully guess the session keys if the PSK is one of the words in the dictionary. If the PSK is short or very simple, it may even be found through a brute-force search [10]. Fourth, WPA Enterprise has *Hole 196 vulnerability*. Hole196 is a fundamental vulnerability in the protocol design, hence Wi-Fi networks using WPA regardless of the authentication (PSK or 802.1x) and encryption (AES) they use, are vulnerable [13],[15],[16]. To exploit Hole 196, a malicious user needs to know the group key (GTK) shared by the authorized users in the WLAN. This vulnerability can be practically exploited using existing open source software such as *madwifi* driver, WPA supplicant, and adding ten lines of code. Its man-in-the-middle attack using ARP spoofing was demonstrated at Black Hat Arsenal 2010 and Defcon18. Other attacks such as port scanning, exploiting OS and application vulnerabilities, malware injection, DNS manipulation and denial of service are possible by misusing GTK [13]. *WPA2* is still the strongest security because of AES encryption and WPA2-PSK authentication. However, like WPA it is not safe. It just takes a longer time to crack AES encrypted packets. WPA2-PSK has the same authentication vulnerabilities of 802.1X as WPA because of PSK [14]. On top of these unencrypted key management and de-authentication problems remain. Moreover, Hole 196 vulnerability alone is a reason why WPA2 security, its encryption, and authentication is unsafe and any access point that uses 802.11ac has security gaps and vulnerable to many attacks [17]. Last, but not the least, and in fact I would brand this vulnerability as the *mother of all vulnerabilities* is the *router backdoor* vulnerability as a result of an open port by default, that has been most probably used by spying agencies. There are a total of 65,535 ports in total, and the port 32764 has been identified as a backdoor port. .It has been revealed that many routers, which are today's popular models from brands such as Cisco, Linksys, and Netgear have the port 32764 open by default using which it is possible for an attacker to hack into the network even from the internet [18].

5 New Recommendations for Solutions

There is definitely a need to design better security mechanisms than what is currently applied in 802.11ac standard wireless routers in WLANs. A few solutions are mentioned in this section (Fig.6). Firstly, manufacturers should get rid of the earlier standards from new routers. A router should not integrate mixed mode (.11ac/n/g/b), but have just one mode for example 802.11ac for security reasons. Weak modes, while providing backwards compatibility, bring in their specific vulnerabilities into the network. Secondly, create routers that only have the strongest security available by default (for example WPA2-PSK authentication and AES encryption) and users should not select any other (remove the drop down list which is used to choose from). Thirdly, design a solution that does not expose SSID before association. Fourthly, design a solution that prevents MAC address from being spoofed. Fifthly, design and implement algorithms in routers that can allow entry of only strong passwords. Sixthly, algorithms have to be designed that takes care of WPA2-PSK authentication and AES encryption vulnerabilities. Seventhly, it would also be of great help if a permanent solution to Hole 196 vulnerability is designed and incorporated in future 802.11 access point standards. Lastly, having all ports on routers closed by default, so that administrators can choose the ports they need to be opened themselves. This will eliminate usage of backdoor ports such as port 32764 which come open by default in many routers and accessible for open access.

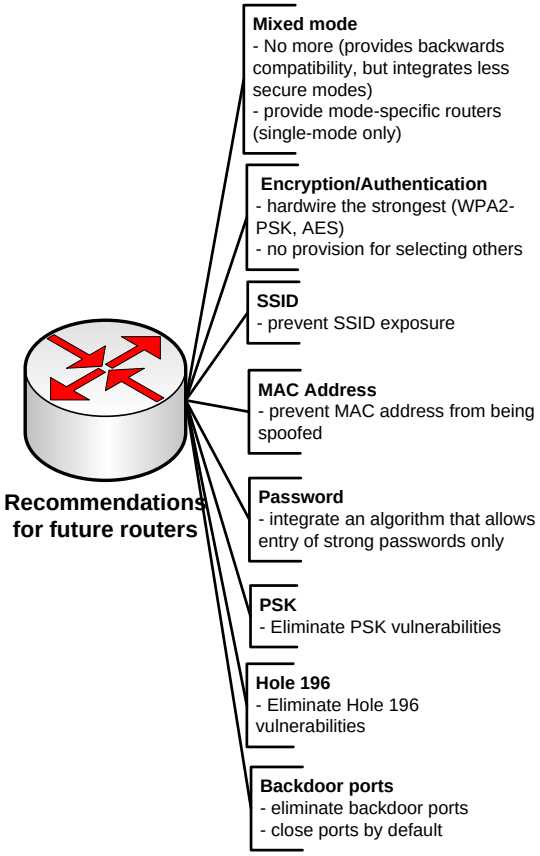

Fig. 6. *Recommendations for Router Solutions*

6 Conclusions

It was seen that 802.11ac standard wireless router provides additional if not better features together with the earlier standards. This paper explained that there is a lot of work to be done in the future in regards to closing persistent security gaps. It has been noted that common earlier security vulnerabilities are still available on 802.11ac routers. These vulnerabilities include SSID vulnerabilities, MAC address vulnerabilities, password vulnerabilities, authentication vulnerabilities, encryption vulnerabilities, and backdoor ports. Overall, the many vulnerabilities or security gaps in 802.11ac routers suggested that the subsequent WLAN environment is still not secured and thus security mechanisms need to be reassessed and redesigned in routers in the future.

References

[1] IEEE-Working-Group, "Official IEEE 802.11 Working Group Project Timelines," IEEE, 2014.

[2] M. Palmer, Hands-on Networking Fundamentals. Boston: Course Technology, 2006.

[3] EC-Council, Ethical Hacking Countermeasures: Secure Network Infrastructures. New York: Cengage Learning, 2010.

[4] N. Dong, "Best 802.11ac routers of 2015," CNET, 2015.

[5] Al Naamany, M. Ahmed, A. Al Shidhani, and H. Bourdoucen, "IEEE 802.11 wireless LAN security overview," IJCSNS, vol. 6, p. 138, 2006.

[6] CompTIA, CompTIA Network+ Certification - Student Manual, 2009 ed. USA: Axzo Press, 2008.

[7] M. Ciampa, "Security+ Guide to Network Security Fundamentals," 4th ed New York: Cengage, 2012, pp. 291-316.

[8] H. D. Lane, "Security Vulnerabilities and Wireless LAN Technology," Sans Institute, 2000.

[9] R. A. Hamid, "Wireless LAN: Security Issues and Solutions," Sans Institute, 2003.

[10] G. Lehembre, "Wi-Fi Security - WEP, WPA and WPA2," Hakin9.org Newsletter, 2005.

[11] A. Pash, "How to crack a Wi-Fi Network's WPA Password with Reaver," in LifeHacker, 2012.

[12] Phillip, "How to Crack WEP and WPA Wireless Networks: Cracking WEP, WPA-PSK and WPA2-PSK wireless security using Aircrack-ng," in SpeedGuide.net, 2008.

[13] Cisco, "Multiple Vulnerabilities in Cisco Wireless LAN Controllers," Cisco Security Advisor, 2014.

[14] Juniper-Networks, "Understanding WPA-PSK and WPA2-PSK Authentication," 13 March 2013.

[15] S. Talegao, "Latest Developments in Wireless Networking and Wireless Security," IOSR Journal of Computer Engineering, vol. 12, 2013.

[16] AirTight-Networks, "WPA2 Hole 196 Vulnerability: Expoits and Remediation Strategies," Whitepaper, 1 April 2014.

[17] A. Tsitrolis, D. Lampoudis, and E. Tsekleves, "Exposing WPA2 security protocol vulnerabilities," International Journal of Information and Computer Security, vol. 6, p. 93, 2014.

[18] M. Horowitz, "How and why to check port 32764 on your router, Defensive Computing, ComputerWorld, 27 Jan 2014.