Campus Area Network Wi-Fi Security

Arjun K. Pillay, Mohammed Farik, Edwin Liava'a

Abstract: Wireless connectivity devices such as mobile phones and laptops are being increasingly used by University students to access learning resources on campus networks and the Internet. Each of the mobile devices offers security protocols for connection to a Wi-Fi router. This paper presents an overview of Wi-Fi security and recommendations in relation to free Wi-Fi service at The University of Fiji.

Index Terms: Router, Security protocol, SSID, WEP, Wi-Fi, WPA, WPA2-PSK

1 Introduction

In recent years, Internet has been increasingly deployed to network devices through wireless fidelity (Wi-Fi) connectivity, namely the IEEE 802.11 standards. Advances in mobile phone technologies have given mobile phones equal if not greater functionality than standard desktop PCs for use of utilities like web browser, media player, Wi-Fi connectivity, and many more. As the advancement of mobile technology and social media increases institutions need to pay more attention to Wi-Fi security issues in order to prevent easy attacks from hackers that can lead to time and financial losses in system repair, unavailability of essential services such as mail and Moodle access by staff and students. Any device that links up to the network becomes part of the network for the connection period. A less secure device will present an easy way for a hacker to launch an attack. If preventive measures are not taken then it will create loop holes for the attackers to launch attacks on network resources via the connected phone. In this paper we will find how securely the mobile devices connect to the Campus free Wi-Fi routers. The outcomes of this research will allow ITC services, network administrators, and network users, also of other similar networks plan better security systems to counter current threats that may emerge via mobile phone connections in Wi-Fi networks. In section 2, we briefly discuss the Campus Wi-Fi services, in section 3, we will discuss the different types of security protocols used in Wi-Fi enabled phones, in section 4, the methodology, in section 5, data collection and analysis, in section 6 recommendations, and finally, conclusions in section 7.

2 Campus Wi-Fi Services

Increase in the number of students allowed the campus to provide free Wi-Fi service to the students. This free Wi-Fi allows certain application to run for example; the student can access search sites, Moodle and student email.

- *Arjun K. Pillay is currently pursing Post-Graduate Diploma program in Information Technology at the University of Fiji. Email: arjunp@unifiji.ac.fj*
- *Mohammed Farik (Member, IEEE) is a Lecturer in Information Technology at The University of Fiji. E-mail: mohammedf@unifiji.ac.fj*
- *Edwin Liava'a is the Manager IT Services at the University of Fiji. Email: EdwinL@unifiji.ac.fj*

On other hand certain application won't be functional such as Facebook, What's app, Viber, and other messaging application. The free Wi-Fi allows students to access internet through their mobile phones, tablet and laptops. Users have to enter manual proxy in order to access internet into their mobile phones. They can then connect to the free Wi-Fi within the campus. Areas covered are in the vicinity of the University canteen, ITS Labs and Library.

3 Wireless Security Protocols

Wireless security protocols provide authentication attempts from a mobile device. The security protocols are WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access and WPA2 (Wi-Fi Protected Access 2) [1]. This security protocol uses different algorithms to secure the transmission of data from point A to point B. Security is a concern as attackers use various types of hacking software and techniques to breach security.

3.1 WEP (Wired Equivalent Privacy)

WEP was the first generation of wireless security protocol which incorporated both encryption and authentication in the IEEE 802.11 standard. It is now considered obsolete due to flaws found in the 802.11 security. WEP uses the standard feature of all 802.11b, 802.11g and 802.11a network equipment [2]. WEP offers Open and Shared key security, and both are weak security protocols. Majority of the smart phones doesn't use the WEP protocol as it is not a reliable security protocol. This is because the WEP key length can be cracked using various tools such as "AirCrack". Also, WEP security protocol uses default values which intruders can attack by using cryptanalysis [3]. This default values can be encrypted using the same IV/WEP combination. IV is the Initialization vector which use combination of secret key to encrypt data. The WEP is also very vulnerable to use in the large organization, since WEP uses short IV's and keys remain static. WEP only uses 24bit key and it uses the same IV for different data packets. If the reoccurrence of the IV increase then the hacker will collect all the frames created using the same IV and the hacker will determine the shared values (KeyStream or Shared secret key) and decrypt any 802.11 frames [1], [4].

3.2 WPA (Wi-Fi Protected Access)

WPA was implemented as a new protocol which was more secure than WEP, this protocol uses 802.1x + EAP (Extensible Authentication Protocol) authentication which is more advance compared to WEP. As seen in Fig.1, WPA uses the two variant methods, namely WPA-PSK (CCMP), and WPA-PSK (TKIP). The authentication method used in this protocol is either CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) or TKIP (Temporal Key Integrity

Protocol). Only CCMP uses Advance Encryption Standard (AES) protocol for data encryption [1], [6], and should be the choice of use. WPA consist of two methods in the authentication part TKIP and MIC (Message Integrity Check) which avoids hackers from accessing the access point in comprise with the hashing method [1]. In TKIP the key dynamically changes (rekeyed) not in the WEP where it has a fixed key, this will make difficult for the hackers to decrypt a packet. The limitations of WPA is that it has compatibility issue regarding the hardware and operating system use and also the using of 256 bit key to generate a string hence it will allow attackers to use brute-force and dictionary attacks [1], [5]. Wireless devices use WPA as the security protocol in order to connect to a Wi-Fi access point. In WPA, users enter password of at least 8 characters which include upper case, lower case, symbols and numbers. However, this password can be cracked using brute-force method.

3.3 WPA2-PSK (Wi-Fi Protected Access Version 2- Pre-Shared Key)

WPA2-PSK protocol is the latest Wi-Fi encryption standard which is implemented to improve security of WPA. WPA2 uses the 802.11i standard feature which consists of data encryption algorithm. As seen in Fig.1, WPA2 also uses the two variant methods, namely WPA2-PSK (CCMP), and WPA2-PSK (CCMP/TKIP). The authentication method used in this protocol is either CCMP or TKIP. However, as in the case of WPA, in WPA2-PSK only CCMP should be the choice of implementation, as it uses AES [1], [6]. Today, most of the mobile devices have WPA2 security feature for connecting to another Wi-Fi device. This security protocol was designed in a way that hackers find it hard to break the encryption. A limitation for using WPA2 is the processing speed. Some researchers mention that using WPA2 requires more powerful hardware to view to maximum network performance for heavy used networks. The issue was regarding using of older wireless access point (WAP) or router [7]. The chances of a hacker to break into WPA2 security using conventional hardware are nil.

4 Methodology

Firstly, Acrylic Wi-Fi Home Go Pro software is used to collect the data from the live UniFiji-Free-WiFi router. This software is the best Wi-Fi analyzer which helps the network administrator to identify access point and Wi-Fi channels, vendors and security protocol each vendor uses [8]. Secondly, the collected data is entered in Weka software to generate descriptive analysis on relevant attributes of Device name, Vendor, and Security. The Device name attribute lists the SSID (Service Set Identifier) name of the devices that have made connection. The Vendor attribute lists the device vendor names. The Security attribute lists the type of security used by each of the connecting devices. The collected data are analyzed and discussed in Section 5 and some recommendations made in Section 6.

5 Data Collection, Analysis and Discussions

Fig.1 shows a section of the screen of Acrylic Wi-Fi Home Go Pro software in its live environment. It shows the 802.11 standard (b, g, and/or n) standards, maximum speed in Mbps, security (WEP, WPA, WPA2), Wi-F- Protected Setup (WPS) availability, and Vendor for each Device (SSID) in connection.

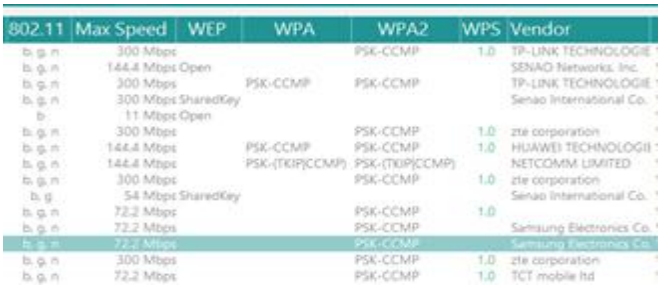

Fig.1 *Part of Acrylic Wi-Fi Home Go Pro*

As can be seen in Fig.2, the Acrylic dataset contains 3 attributes of Device Name, Vendor, and Security. A total of 29 records (instances) are present for analysis purposes.

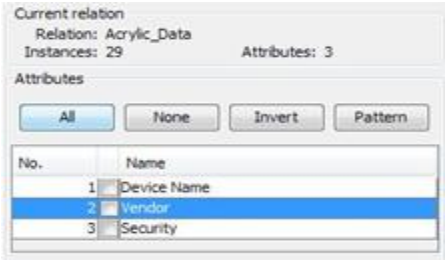

Fig.2 *Acrylic_Data in Weka for Analysis*

Fig.3 shows the Names or SSID of devices that are in connection. There are 13 distinct SSIDs which accounts for only 41% of connections. 51% of the SSIDs in the dataset use the same SSID “Android AP”, which is a default SSID. There is a chance that this SSID was broadcasted by the same device. However, there is also the chance that SSID was broadcasted from different devices. It is highly recommended that this default SSID is edited or changed by the device owners to avoid confusion. The SSID can be formatted as for instance “Android AP s100144”, where Android AP is default SSID and s100144 is student’s university identification number. This will also make it easier for network administrators to identify which student is currently in connection to Wi-Fi service.

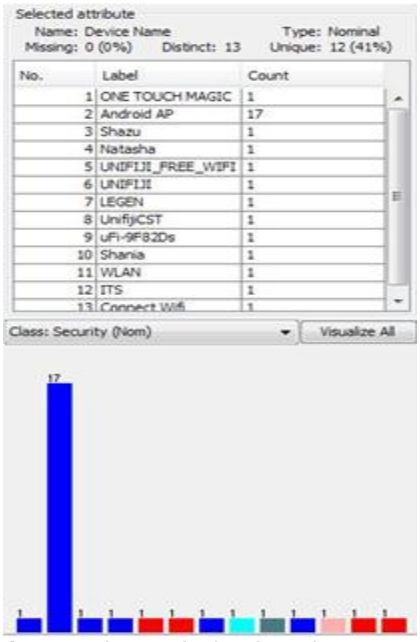

Fig 3. *Weka Analysis of Device Names*

Fig. 4 shows that the most common vendor of the connecting devices is Samsung. These have been identified as belonging to SSID or device name Android AP. TP-LINK, SENAO, NETCOM are other active WAPs. This information on Vendor acceptability by users can help the ICT services on planning for network upgrades and expansions that is relevant to this majority category of user base. Best practices and services from this vendor and device name can also be negotiated in future for this group for their customer loyalty to Samsung and its Android AP Wi-Fi device (phone), for example. Fig. 5 shows that 22 out of the 29 devices connected using WPA2-PSK security, which is the best security available today. Most of this best security relates to Device Name Android AP and Vendor Samsung. 3 others used at least WPA, whereas 4 devices used WEP for connectivity. While 4 is a small number, it should be noted that a single weak spot for hacker entry can cause major damage to network resources. From Fig.1 it can be seen that WEP is configured on SENAO devices. These devices are WAPs configured and managed by IT Services. It is better to replace these devices if the highest security is unavailable on these devices. If the option is available, but is not configured for easier connectivity reasons, a better solution is recommended in the next section.

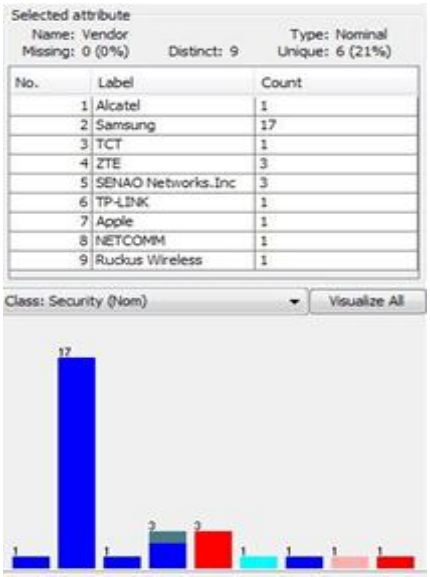

Fig 4. *Weka Analysis of Vendors*

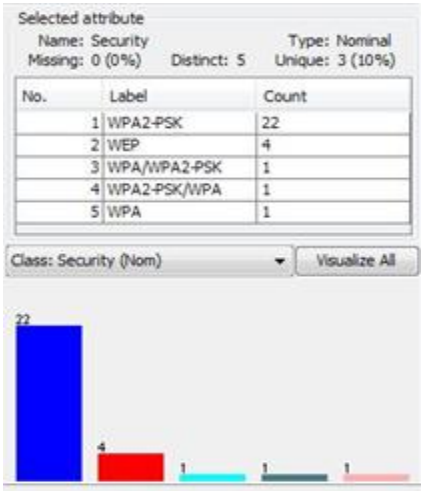

Fig 5. *Weka Analysis of Security*

6 Recommendations

First, we believe the best security, WPA2-PSK should be priority number 1 in network issues. Whatever the reasons, security should not be compromised. The IT Services should first upgrade or configure its WAPs for WPA2-PSK security. It needs to also carefully monitor what kind of phone or laptop is connecting to its WAPs. While the free software tool Acrylic Wifi Home Go Pro was used in this research, another good choice would be to use Kali Linux, a Debian-derived Linux distribution which is designed for digital forensics and penetration testing. Second, provide Wi_Fi connectivity free or otherwise only via WPA2-PSK configured settings and devices. Better still register the users, and configure their devices at IT Services. We recommend changing the SSID to student or staff identification numbers, and allowing only these to establish connection. This will allow IT Services to be aware of as to exactly who is on the network at a given time. Also, this way network issues in relation to specific users can be dealt with on an individual basis. Third, the user needs to enter a strong password in configuring his/her WPA2-PSK mobile phone. Forth, if phone or laptop wishes to establish connection using WEP security, it should be denied access for security reasons. Fifth, vendors should configure the highest security in their wireless devices by default, preferably WPA2-PSK. Lastly, the vendors need to emphasize on the security aspect of their wireless devices and create awareness through their user documentation of their products.

7 Conclusion

IT is seen that the campus area network's Wi-Fi is not secure and can be attacked by hackers due to relaxed security configurations in a few WAPs. However, the positives are that a vast majority of users are connecting to WAPs using the highest WPA2-PSK security protocol via latest Samsung android phones. This gives new opportunities to IT Services to exploit this trend.

References

[1] M. Farik and S. Ali, "Recurrent Security Gaps in IEEE 802.11ac Routers," International Journal of Scientific and Technology Research, vol. 4, no. 9, 2015.

[2] A. Sari and M. Karay, "Comparative Analysis of Wireless Security Protocols: WEP vs WPA", International Journal of Communications, Network and System Sciences, vol. 8, no. 12, pp. 483-491, 2015

[3] R.Schenk,"Wireless LAN Deployment and Security Basics". PCMAG, 2017. [Online]. Available: http://www.pcmag.com/article2/0,2817,1157727,00.asp. [Accessed: 05-Jun-2017].

[4] Wi-Fiplanet.com, "802.11 WEP: Concepts and Vulnerability", Wi-fiplanet.com, 2017. [Online]. Available: http://www.wi-fiplant.com.tutorials/article.php/1368661/80211-WEP-Concepts-and-Vulnerability.htm. [Accessed: 05-Jun-2017].

[5] Brighthub.com, "Advantages and Disadvantages of WEP WPA Network Security", Bright Hub, 2017. [Online]. Available: http://www.brighthub.com/computing/smb-security/articles/78216.aspz. [Accessed: 06-Jun-2017].

[6] Whirlpool, “Encryption – WEP and WPA”, Whirlpool.net.au. 2017. [Online]. Available: http://whirlpool.net.au/wiki/wlanh_103. [Accessed: 31-May-2017].

[7] Differencebetween.net, “Difference Between WPA and WPA2 | Difference Between”, Differencebetween.net, 2017. [Online]. Available: http://www.differencebetween.net/technology/difference-wpa-and-wpa2/. [Accessed: 06-Jun-2017].

[8] Acrylicwifi.com, “WiFi analyzer – Acrylic Wifi professional for windows”, Acrylic Wifi, 2017. [Online]. Available: https://www.acrylicwifi.com/en/wlan-software/wifi-analyzeer-acrylic-professional/. [Accessed: 31-May-2017].