Article 3

RaspyAir: Self-Monitoring System for Wireless Intrusion Detection using Raspberry Pi

Mohd Nizam Osman, Mohd Syafiq Aiman Mohamad Zulrahim
Faculty of Computer & Mathematical Sciences
Universiti Teknologi MARA Perlis Branch

Mushahadah Maghribi
Department of Information Technology and Communication, PTSS Perlis

Abstract
This paper described a self-monitoring for wireless intrusion-detection system (IDS) using Raspberry Pi to enhance the security performance for personal computers. Nowadays, most of the personal computers are interconnected without wire. Therefore, everybody can easily connect to the Internet and indirectly exposed to the security issues, especially the safety of the confidential data. Sometimes, we do not know that someone is sniffing our network, even we do not realize that there was an intruder in our network due to most of the personal computers does not have the intruder monitoring system. To overcome this problem, we proposed a system for wireless monitoring and intruder detection for personal computer known as RaspyAir. This system was implemented using misuse detection approach, which is hybridization of tShark and Airodump-ng to capture the possibility of the traffic in the wireless environment. The brute-force algorithm is used to filterthe traffic using signature based detection technique. Then, RaspyAir was integrated with a credit card size single board computer, which is Raspberry Pi as an external tool for monitoring system. The developed system is then tested using code auditing and penetration testing to identify the achievement of the system. After applying the testing from Wireless Security Assessment Methodology (WSAM), a standard measure score is calculated to evaluate the degree of the security for the system. Hence, the result has shown the RaspyAir followed the security guidelines, fully secured, can be deployed for personal computer and significantly increase the security performance for monitoring wireless intrusion-detection system. Additionally, from the experiment conducted has confirmed that by using Raspberry Pi as an external tool, it consumed nine times less electrical power compared to the personal computer.

Keywords*: Wireless, intrusion detection system (IDS), monitoring system, wireless security assessment methodology (WSAM), Raspberry Pi.*

Introduction

In recent years, wireless networking has been experiencing an explosive growth, which resembles the rapid growth of the Internet itself in the mid-1990s. According to the report by International Telecommunication Union (ITU), almost 40 percent of the world population has an internet connection (ICT Data and Statistics Division, 2015). Furthermore, wireless networking is the easiest way to set up an internet network. There are no obtrusive cables, and people are free to use

their devices virtually anywhere in the coverage area. In addition, new devices can be added to the network just in minutes.

Nowadays, the wireless network becomes a necessity. In essence, a wireless network lets multiple devices in the coverage area, share the same broadband Internet connection, as well as talk to one another. The most common type of Internet network in today's home/work is a wireless network or also known Wi-Fi. At present, the range of Wi-Fi network is about 30-40 metres indoor and up to 100 metres outdoors. Besides, a high-powered Wi-Fi standard known as 802.11y is intended to boost outdoor up to 5000 metres, enabling for increased wireless operation for more users at much higher power than via traditional Wi-Fi equipment.

Connecting network to the internet access provides access to the huge amount of information. It allows people to share information across the globe. However, common nature of the Internet, which creates so many benefits, also offers the malicious users to access giant amount of targets. For this reason, an unsecured wireless network gives hackers the perfect gateway to access to a personal computer or an organization's internal network. Besides letting the hacker steal or destroy information on the network and giving him or her free Internet access, then the wireless network might also help him or her to carry out cyber-attack. Hence, this situation will make internet users vulnerable to data security risks. Indeed, since there is no way to identify a hacker on a network from the personal computers, which installed the wireless network, might be opened to the attack. Therefore, the users have responsibility to ensure the safety of the network from the intruder, especially on the security issues. This issue should be resolved by identifying the main causes, which most of the problems relate with the users who using the wireless network. Besides, the number of users using the wireless network tremendously increasing, then each user must have a monitoring system for wireless intrusion detection, which can be installed on the personal computer to monitor every activity occurs on the network.

Network monitoring activity refers to the ability of the system to notify the network administrator if there are failed in devices, and outage occurred in the network by monitoring the device to see the network traffic and log the information of network traffic (Zargar, Joshi, & Tipper, 2014). This is crucial for the network in order to analyse the performance and security of the network system. To observe the performance of the network, the performance metric are being used. For instances, throughput, average latency, bandwidth consumed, average delay, and mean batch service time. Meanwhile, network security is important to ensure the availability, confidentiality and integrity of the data transmission. There is a research conducted to study about network security of wireless home network and the result shown there were a lot of foreign IP addresses found in the traffic (Aspernäs & Simonsson, 2015). Therefore, it was confirmed that unauthorized users who are currently connected to the access point without us realizing it. Hence, the network performance will decrease because of massive traffic by unauthorized users.

On the other hand, the intrusion detection is the mechanism to detect any unusual network traffic and notify the user to take action. The unusual network traffic usually caused by the malicious user who sending out illegal packet to the network for any purposes. Hence, it will increase the respond of user to take action and prevent the threat from reaching the network resources. To overcome the problems, there must be some computer algorithms to analyse the pattern of the

network traffic. There are varieties of approaches(Dmitry & Dennis, 2008; Jia & Chen, 2009; Makanju, Zincir-Heywood, & Milios, 2008) in the intrusion-detection system (IDS), which are behavioural, signature and combination of both. For instance, misuse detection use signature analysis of the network traffic by defined the lawless action and compare it with the observed object or based known system bug and intrusion pattern (Jia & Chen, 2009). Other researchers use collaborative intrusion, which combines many detection approaches (Mingqiang, Hui, & Qian, 2012). The advantages when using the collaborative intrusion-detection system, repairs some drawback of traditional cluster algorithm and achieving satisfaction performance. Unfortunately, the complexity of the algorithm caused of memory requirement and growth in the record number. On the other hand, collaborative IDS also cooperate with mobile agent and applying them into the intrusion-detection system, which an autonomous agent can provide the suitable, systematic and strong programming paradigm for shared application (Mo, Ma, & Xu, 2008). This approach reduces central processing unit (CPU) and memory usage.

There are varieties of techniques used in order to monitor the wireless intrusion detection. For instance, intrinsic monitoring which relies on IP extension headers in combination with formal behaviour models to gather information along the path in order to delegate monitoring functionality to the network devices (Höfig & Coşkun, 2009). Besides, G. Song (2012) uses two structures of the monitoring system, which are data display module and traffic monitoring module and make the monitoring system can monitor traffic in more than one computer, reduce the workload of network management and improve network traffic monitoring (Song, 2012).

As the technology becomes sophisticated, the wired connection moves to wireless connection and this technology widely used around the world. However, there were a lot of flaws associated with the wireless protocol that will attract the cyber-criminal to penetrate the network. For instances, it is possible for the malicious users to eavesdropping the communication in the wireless network and abuse the information. Hence, it is essential to have a system that can monitor for the wireless intrusion detection for all users. Moreover, the intrusion-detection system that existed today was integrated with the large scale of hardware.

Therefore, a save cost device is needed, and it can easily attach to the wireless network without any specific space configuration. Hence, we developed a self-monitoring system for wireless intrusion detection using Raspberry Pi as an external tool to enhance the security performance of the wireless network. Raspberry Pi is a single board computer, and it also can make any computational process for many applications (Agrawal & Singhal, 2015; Paramanathan et al., 2014; Soetedjo, Ashari, Mahmudi, & Nakhoda, 2014). There is a research conducted using Raspberry Pi as the intrusion-detection system with some limitations such as suffering lower network throughput(Aspernäs & Simonsson, 2015). The advantage of Raspberry Pi, it can operate same as computer but in small version and more interactive besides consumed less electricity.

Methodology

The study starts by studying previous research, journal, book and website that use intrusion-detection system (IDS) and monitoring system for wireless environment. From this study, a set of the guideline was produced to develop the monitoring system for wireless intrusion detection using

Raspberry Pi (RaspyAir). This guideline mainly concerns with the intrusion-detection system, monitoring system, wireless technology and Raspberry Pi.

While developing the prototype, the RaspyAir used misuse detection approach. This approach was implemented signature based detection technique, which means that they operate by searching for a known identity or signature for each specific intrusion event. For that, all the network traffic will be filtered using brute-force algorithm and gave an alert to the user if an intruder detected. The network traffic is captured by using TShark and Airodump-ng. Besides, the RaspyAir was designed with two types of network analysis, which are real-time analysis and offline analysis. The real-time analysis is an analysis based on the current state of the wireless network, whereas the offline analysis is an analysis based on input of wireless traffic files type such as *.pcap* and *.cap*. Then, the RaspyAir will generate a report to the user, and user can simply print the report for future use.

After the development phase,the RaspyAir will be tested to identify the achievement of the security performance. This study conducts the penetration of testing, where the specific attacks will be launched to the system. The security testing of the system was done using Wireless Security Assessment Methodology (WSAM) by Karthik (2015). This is to ensure that the RaspyAir can provide a secure application.

WSAM provides a guideline for setting up a security standard, checking compliance, gathering firmware version for all types of devices, finding unapproved access point, checking if decoded movement is navigating the remote system and guaranteeing that feeble types of WEP (Wired Equivalent Privacy) are not being used. The assessment was made based on five types of attack, which are availability, access control, confidentiality, integrity and authentication attack (Karthik, 2015).
To have a standard measurement, score values for the attacks are defined in Table 1.

Table 1: Score value for the attack evaluation

Score Value	**Scoring Meaning**
1	Not Secure
2	Partly Secure
3	Fully Secure

At the end of testing, all scores will be summed up and the percentage will be calculated. This percentage will be analysed to determine whether the RaspyAir is secure or not. Table 2 represents the meaning of percentage in order to get the result or conclusion of the research for the RaspyAir.

Table 2: The definition of the security percentage calculated

Percentage	**Definition**
Less than 25%	The system failed to meet the guideline requirement for the types of attack.
26% - 50%	The system meets some of the guideline and helps eliminate some vulnerability but still need a lot of improvement.

51% - 79%	The system meets most of the guideline and is adequate to build a wireless security system.
80% - 100%	The system meets the guideline requirement and helps to build a good wireless security system.

Then, the overall percentage was calculated to classify whether the RaspyAir follows the security guideline or not and to determine whether the system developed can be deployed or not. Table 3 shows the meaning of the overall percentage towards the acceptance of the proposed system.

Table 3: The definition of the overall security percentage calculated

Percentage	Definition
Less than 50%	The system cannot be used and need a lot of improvements.
51% - 75%	The system can be used but partly secured and must be monitor by the developer.
76% - 100%	The system followed the security guidelines and fully secured. Therefore, it can be deployed.

Finally, the electricity consumption testing has been conducted to compare the electricity consumption between Raspberry Pi and HP Compaq Notebook. In order to measure the electricity consumption of the two computers, a Multifunctional Mini Ammeter was used.

Security Evaluation

The five different types of attack as suggested by the WSAM guideline were evaluated. The first attack is access control attack, which focuses on penetrating the wireless by evading the wireless security measure such as MAC filter and Wi-Fi port security to obtain unauthorized access. The second attack is wireless integrity attack which the attacker sends modified control, data and management frame over the wireless network to misdirect the wireless devices in order to perform denial-of-service(DoS) attack. The third attack is confidentiality attack focuses on interception over the wireless network either in clear plain text or encrypted by Wi-Fi protocol. The fourth attack is availability attack prevents the legitimate user from accessing the access point via access point(AP)theft, beacon flood, authentication flood, temporal key integrity(TKIP) message integrity code(MIC) exploitation, de-authenticate flood, routing attacks Address Resolution Protocol(ARP) cache positioning and power saving attacks. Finally, we evaluate on authentication attack which the purpose is to steal identity information of Wi-Fi clients and to gain unauthorized access of the wireless network resources which can be happened over a course of time through application login theft, preshared key(PSK) cracking, shared key guessing, domain login cracking, identity theft, virtual private network(VPN) login cracking, lightweight extensible authentication protocol (LEAP) cracking and password speculation.

Research Results

To evaluate the security degree of RaspyAir, the study has successfully done fifteen attacks in the area of access control attack, wireless integrity attack, confidentiality attack, availability attack and authentication attacks on the home/work wireless network. Basically, the work involved

finding the security bugs in order to evaluate the system. The score value was given for every type of attacks launched. Table 4 shows the score value.

Table 4: Wireless Security Evaluation Result

No.	Attacks	Score (1 - 3)
Access Control Attack		
1	Rough access point	3
2	Probing by wireless devices	3
3	Evil twin	3
Total		**9/9**
Wireless Integrity Attack		
4	ARP request replay	2
5	WPA Bruteforce	3
6	KorekChopChop	3
7	Fragmentation	1
Total		**9/12**
Confidentiality Attack		
8	WEP key cracking	2
9	WPA migration mode attack	3
Total		**5/6**
Availability Attack		
10	WPA attack	3
11	WPA migration attack	3
12	Mdk3 Michael shutdown	2
13	Beacon flooding	3
Total		**11/12**
Authentication Attack		
14	Authentication Dos	3
15	Association flooding	3
Total		**6/6**

The study has successfully done for each type of attack. Table 4 summarized the results for the identified area, and Table 5 represented the percentage of security testing. For the area access control and authentication attacks, with a result of 100%, we found that the system meets the guideline requirement and helps immensely in building a secured wirelessintrusion-detection system. Meanwhile, testing the security in the area of confidentiality and availability, with a result of 83% and 92% respectively, shown the system meets the guideline requirement and helps to build a good wireless intrusion-detection system. Hence, it proved that, these types of signature attack can easily recognize by the RaspyAir. On the other hand, the percentage for integrity attack was 75%, showed that this type of attack cannot easily be detected by RaspyAir. This is most probably because this type of attack used different type of parameter from the RaspyAir system.

Table 5: Percentage of the security testing

Attack Types	Score	Percentage
Access Control	9/9	100%
Integrity	9/12	75%
Confidentiality	5/6	83%
Availability	11/12	92%
Authentication	6/6	100%
Overall Percentage		88.89%

Table 5 shows the overall percentage was 88.89%, and it described that the RaspyAir followed the security guidelines and can be deployed on the wireless environment.

Table 6: Electricity consumption for both devices

	HP Compaq Notebook	Raspberry Pi
Electricity consumption (kWh)	0.0419	0.0045
Electricity cost (RM)	0.01	0.00

For the second testing, which is electricity consumption testing, found that the electricity consumption for Raspberry Pi which is 0.0045 kW was lower than HP Compaq Notebook, which is 0.0419 kW. Moreover, the electricity cost in two hours period for Raspberry Pi also lower than HP Compaq Notebook. Table 6 shows the electricity cost and consumption for both devices.

Conclusion

In this paper, we have presented the RaspyAir for home/work wireless environment. The system was specifically developed for monitoring the wireless intrusion detection for personal computer. The system used Raspberry Pi as an external tool to enhance the security performance of the personal computer. The used of Raspbery Pi and the RaspyAir system provide most economical and enhance the security performance for wireless intrusion detection. The advantage of RaspyAir due to the system is installed in an external tool and if anything happened, it will not harm the personal computer directly. Hence, the system provides a convenience way of monitoring the security level through the use of Raspberry Pi. Besides, the RaspyAir was evaluated using WSAM guideline and the result shown the RaspyAir followed the security guidelines and can be deployed on the wireless environment. Additionally, the electricity consumption of the RaspyAir was proved nine times saved than HP Compaq Notebook, likewise, the electricity cost for Raspberry Pi. The result of all criteria that was evaluated indicated that the RaspyAircontributes significantly in monitoring system for wireless intrusion detection for personal computer.

References

Agrawal, N., & Singhal, S. (2015). Smart drip irrigation system using raspberry pi and arduino. In *2015 International Conference on Computing, Communication Automation (ICCCA)* (pp. 928–932).

Aspernäs, A., & Simonsson, T. (2015). *IDS on Raspberry Pi: A Performance Evaluation*. Diploma thesis, University of Delaware.

Dmitry, S. K., & Dennis, Y. G. (2008). Network traffic analysis optimization for signature-based intrusion detection systems. In *Proceedings of the Spring/Summer Young Researchers' Colloquium on Software Engineering*.

Höfig, E., & Coşkun, H. (2009). Intrinsic monitoring using behaviour models in ipv6 networks. In *IEEE International Workshop on Modelling Autonomic Communications Environments* (pp. 86–99).

ICT Data and Statistics Division. (2015). *ICT Facts & Figures The World in 2015*. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf

Jia, C., & Chen, D. (2009). Performance evaluation of a collaborative intrusion detection system. In *2009 Fifth International Conference on Natural Computation* (Vol. 6, pp. 409–413).

Karthik, P. (2015). *Wireless Security Assessment Methodology* (Whitepaper) (pp. 1–7). Retrieved from ww.happiestminds.com/whitepapers/Wireless-Security-Assessment-Methodology.pdf

Makanju, A., Zincir-Heywood, N., & Milios, E. (2008). Adaptabilty of a GP Based IDS on Wireless Networks. In *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on* (pp. 310–318).

Mingqiang, Z., Hui, H., & Qian, W. (2012). A graph-based clustering algorithm for anomaly intrusion detection. In *Computer Science & Education (ICCSE), 2012 7th International Conference on* (pp. 1311–1314).

Mo, Y., Ma, Y., & Xu, L. (2008). Design and implementation of intrusion detection based on mobile agents. In *IT in Medicine and Education, 2008. ITME 2008. IEEE International Symposium on* (pp. 278–281).

Paramanathan, A., Pahlevani, P., Thorsteinsson, S., Hundeboll, M., Lucani, D. E., & Fitzek, F. H. P. (2014). Sharing the Pi: Testbed Description and Performance Evaluation of Network Coding on the Raspberry Pi. In *2014 IEEE 79th Vehicular Technology Conference (VTC Spring)* (pp. 1–5).

Soetedjo, A., Ashari, M. I., Mahmudi, A., & Nakhoda, Y. I. (2014). Raspberry Pi based laser spot detection. In *2014 International Conference on Electrical Engineering and Computer Science (ICEECS)* (pp. 7–11).

Song, G. (2012). The study and design of network traffic monitoring based on socket. In *Computational and Information Sciences (ICCIS), 2012 Fourth International Conference on*(pp. 845–848).

Zargar, S. T., Joshi, J., & Tipper, D. (2014). DiCoTraM: A distributed and coordinated DDoS flooding attack tailored traffic monitoring. In *Information Reuse and Integration (IRI), 2014 IEEE 15th International Conference on*(pp. 120–129).