INBOUND TIME STAMPING FOR DETECTING ROGUE ACCESS POINT

Amran Ahmad[1], Suhaidi Hassan[2], and Mohd Hasbullah Omar[3]

[1]Universiti Utara Malaysia, Malaysia , amran@uum.edu.my
[2]Universiti Utara Malaysia, Malaysia, suhaidi@uum.edu.my
[3]Universiti Utara Malaysia, Malaysia, mhomar@uum.edu.my

ABSTRACT. Rogue Access Point (RAP) is a network vulnerability phenomenon of improper usage of wireless Access Point unknown to an organizational network engineer. Once it is inside the subnet or Local Area Network (wired structure) then we need to rectify of its availability. The process of rectifying can be classified into passive monitoring, using visualization and traffic characteristic. We prefer traffic characteristic scanning where a packet capturing can become one of the best tools to differentiate between wired and wireless network. Our main concentration is time stamping as a value added to packet capturing for wired and wireless differentiation. The time stamping is done at two point inbound inside subnet focusing on a PAYLOAD and its ACK using network test bed measured by finding an average of 100 PAYLOAD-ACK pairs. The test show about 16 to 56 percent differences between wired and wireless g mode and 15 to 26 percent differences between wired and wireless n mode. As a result, it shows that there is more delay on wireless than the wired and easier for us to detect RAP existence in wired network.

Keywords: RAP, inbound time stamping, PAYLOAD-ACK pair

INTRODUCTION

The number of Internet users is increased lately. The rise of web 2.0 also invites many web developers to develop a new and sophisticated web services which can attract users to visit Internet frequently. Instead of the phenomenon, we are also being given choices to connect into Internet; either using wired or wireless.

The concept of mobility is already known to many users especially the on moving businesses and also normal users. The most versatile device used for communication like hand phone is not for trendy anymore. It is already become a standard where the accessibility to Internet also done through wireless. Some of them connected through Access Point (AP) instead of other services like 3G or 4G.

Some organization also prefers using AP for extending their network. We believe the device that owned by the organization is properly setup however some staff who have more than one computer and sitting at a poor coverage area will choose to plug their own AP to the nearest data point (wired). This is where the Rogue Access Point appears in the organization.

Rogue access points (RAPs) expose the enterprise network to network vulnerabilities and normally connected to the network behind the firewall (Beyah, Kangude, Yu, Strickland, & Copeland, 2004; Gao, Corbett, & Beyah, 2010; Han, Sheng, Tan, Li, & Lu, 2011; Sriram, Sahoo, & Agrawal, 2010). Unauthorized RAP produce security vulnerabilities in organization networks by circumventing inherent security mechanisms (Ma, Teymorian, & Cheng, 2008; Hou, Beyah, & Corbett, 2007) and installed on a secure network without the explicit permission of the appropriate network management authority (Schweitzer, Brown, & Boleng, 2007).

The popularity of the 802.11-based Wireless LAN (WLAN) also increases its risk of security attacks such as Denial of Service (DoS) attacks (Liu & Yu, 2008). This is happen due to an open medium, insufficient software implementations, potential for hardware deficits, and improper configurations (Ma et al., 2008). Even though APs are a best extensible device for network advancement, but it is also a main contributor to network vulnerabilities if it is connected without proper security configuration (Srilasak, Wongthavarawat, & Phonphoem, 2008).

There are certain approach how RAPs can be prevented such as using passive monitoring, traffic analysis and comparing different traffic characteristic. Those three approaches are discussed in this paper.

From the three we put our effort more on traffic characteristic analysis through Time Stamping technique. This technique depends on packet capturing mechanism which will capture at two different points and based on PAYLOAD-ACK pairs flag. The two captured point then summarize for concluding the different time between wired and wireless access. In this paper we only focus on the time stamping technique that can be a part of the overall solution for detecting RAP by comparing the packet from wired and wireless. The differences will help us to find the RAP devices connected to LAN (wired). The next section will discuss the previous work that related for detecting RAP.

PREVIOUS WORK

The existing of RAP in network environment is a worst case scenario. Even though the network is robust with high-end security mechanism, RAP will break the security bridge and open the network services to any user. In our case, detecting RAP is becoming the first priority than denying it existent. Some related works had been done and can be categorized into three different categories as stated below.

Passive monitoring

The packet flowing for both wired and wireless have a different characteristics. It can be distinguished by using algorithm for computing Round Trip Time (RTT) (Hou et al.2007). Monitoring should immediately take place at switch near to AP. The different between wired and wireless RTT can be seen and RAP can be detected using the algorithm. Another approach was proposed by (Wei et al., 2007); consist of two different algorithms with training or without training using sequential hypothesis testing. This technique use to capture packet header and TCP ACK–pairs are analyzed within the data. Both algorithms have exploited the fundamental properties of 802.11 CSMA/CA MAC and half duplex wireless channel to find the different between wired and wireless network.

Using visualization

The most skeptical part for identifying RAP is it location. Detecting the existing of RAP is not difficult comparing to identifying the place where it is placed. (Schweitzer et al., 2007) used ‘profile mapped’ to detect any RAP by analyzing the strength of wireless signal receive by legal AP. In addition, the data use to plot the map. RAPs will be discovered on the map.

Traffic characteristic

There are three kind of traffic characteristic (Beyah et al., 2004): One to one corresponding, link speed and inter packet switching. One to one corresponding where one MAC address is for one device. If detected differently than the traffic is sending by AP. The next stage is to trace either it is RAP or otherwise. Link speed also gives a different measurement. For Ethernet, the switch can have about 100 MB whereas 802.11 g have about a half. The different between wired and wireless also can be detected through inter packet switching. It is also related to the correspondent between clients with APs or other devices. It is may be in the form of one IP with one MAC or many IPs with one MAC. From the packet those information can be gained and analyzed.

We create our time stamping approach by combining executing packet capturing. The packet capturing is consisting of time stamping approaches which will stamps the PAYLOAD-ACK pairs between Host and Server. It is done at inbound where it is easily being control than outbound where more consisting of more than one hops. The next section will highlight the time stamping mechanism that we used to rectify RAP.

METHODOLOGY

We divided our processes into two sections: packet capturing and time stamping. As all of us concern, our time stamping structure is sitting inside the packet capturing mechanism. Each packet captured that comprising of PAYLOAD and the PAYLOAD ACK then time stamp. Our next discussion is focusing on these two topics; packet capturing and time stamping.

Packet Capturing

Packet capturing that we choose is already have all the features that complying with our needs. It is injected into our time stamps structure to become a front structure for capturing the packet flowing from host to a router. Packet capturing is handled by PCAP mechanism in four processes:

1. Interface to capture should be rectified in two conditions, specify or let system decided what interface is available at the machine and choose to be captured. Consequently, we may optionally provide other parameters to make the capture more reliable and accurate towards our objective.
2. After the interface is stated then an initialization process begins. It will scope the capture to the specific parameters and a session it is created to start the job.
3. The parameter that we discuss previously is called rule (TCP-ACK pair) which compile and execute by PCAP and become a filter. The rule is kept in a string then converts into PCAP format and applies it to the specific session that being created just now.
4. Lastly, the PCAP enter into its execution loop and start capturing network packet.

This ensures that the process is repeated until users interrupt the process with specific command. While capturing, the packet is filtered into TCP-ACK Flag. At this filtering stage, out time stamping process will measure the differences between PAYLOAD and its ACK. This flag is a special flag because it shares with the normal ACK flag. Payload is the ACK that have a data (Data field is non-zero). It is send by server to host which is requesting it through PUSH flag. As usual the successful Payload is acknowledged.

The packet capturing engine will execute at the router and waiting for TCP segments to arrive and captured. The captured will happen at subnet interface only where the number of hops is known. Consequently, we are not going to focus on interface at the Internet side (outbound) because the number of hop is not known and uncontrollable.

Time Stamping

This process is launched after the PAYLOAD packet is captured and identified (see Figure 1).

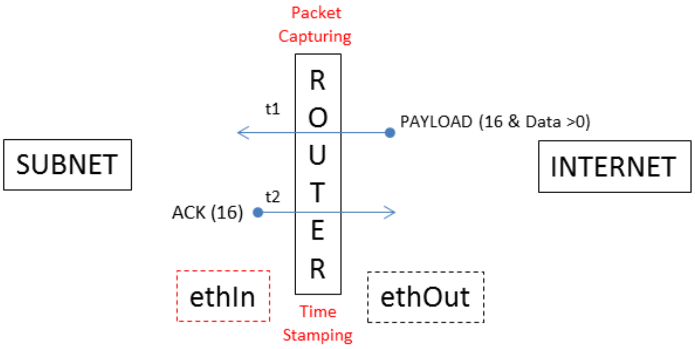

Figure 1. Packet Capturing and Time Stamping

This task is to time stamp two different times between PAYLOAD with its ACK. According to figure 1, the two times stamp are showed by t1 and t2. The t1 represent PAYLOAD whereas t2 represent ACK. The t1 and t2 is paired through an equality of SEQ number with ACK number and then a time different is calculated to measure a time spent from t1 to t2. This difference will be used to detect RAP.

Experimental Setup

We developed network test bed for evaluating our time stamping approaches (see figure 2).

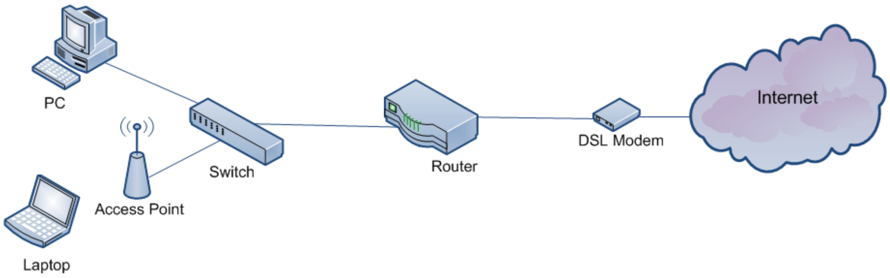

Figure 2. Network Test bed

The requirement of our RAP detection experimental setup is divided into two; hardware and software. The hardware requirements are listed below.

1. Router - This is our main subject where the time stamping structure is deployed.

2. Hosts - This is the end point and easy to plug into the network.

There are no specific specs that we set and the most important things it is connected and can start requesting information to any destination (Internet). We consider both OS platform which are Linux and Windows. Furthermore, the observation is pointing to both wireless g and n modes for finding the differences between both wireless modes to the wired connection. Instead of hardware above, we need a list of software to complement our hardware.

1. Ubuntu 11.04 Server Edition - Running DHCP server, Firewall and Network Address Translation (NAT).

2. C language - Our Packet Capturing that support time stamping mechanism are developed using this language.

The experiment executes using two hosts, each connected to wired and wireless. We try to be equal between the two Hosts by accessing the same sources through macro that already being recorded. The macro will start at same time and repeating the same sequences until an hour. The next section will go through our real capturing and time stamping for seeing the different between wired and wireless access. The result is discussed in a next topic.

RESULT

As describe above, the one hour experiment of capturing and stamping done through our network test bed. Whatever packet will be captured but only PAYLOAD and its ACK are stamps. For validation purposes, we take five data sets of 100 differences of PAYLOAD-ACK pair from two different wired and wireless (g and n modes) networks. The sets are analyzed for evaluating either our process can be used to distinguish between wired and wireless (where RAP is placed).

Table 1. Time Stamp Result

Data Sets	Wired (ms)	Wireless (ms)	
		g	N
1	0.004934	0.030019 16%	0.033806 15%
2	0.004943	0.019933 25%	0.031653 16%
3	0.004920	0.008826 56%	0.033560 26%
4	0.001959	0.005693 34%	0.028743 20%
5	0.002771	0.009937 28%	0.039364 25%

The datasets (wired and wireless) is summation and divide by 100 for getting an average (see Table 1). The average of wired are between 0.001959 and 0.004943 ms whereas the average of wireless g mode are between 0.005693 and 0.030019 ms. Meanwhile the average of wireless n mode are between 0.028743 and 0.039364 ms. As a result the percentage of differences from wired to wireless (g and n modes) are derived where the result shows about 16 to 56 percent (wireless g) and 15 to 26 percent (wireless n).

CONCLUSION

The availability of RAP is not welcoming to the network environment. It will bring vulnerability especially to private data. We propose the combination of packet capturing and time stamping at two different points at inbound inside network subnet. This is easy to control than time stamping at outbound. From the various TCP flags, we choose PAYLOAD and its ACK to be time stamped. The experiment shows from five data sets of 100 PAYLOAD-ACK pair, the different of wired to wireless g and n modes is about 16 to 56 percent (wireless g) and 15 to 26 percent (wireless n). This concludes that our mechanism can be used to distinguish between wired and wireless network. Hence, this different can be used to rectify the availability of RAP in wired environment.

REFERENCES

Beyah, R., Kangude, S., Yu, G., Strickland, B., & Copeland, J. (2004). Rogue access point detection using temporal traffic characteristics. *Global Telecommunications Conference*, 2271-2275. doi: 10.1109/GLOCOM.2004.1378413

Gao, K., Corbett, C., & Beyah, R. (2010). A passive approach to wireless device fingerprinting. *Dependable systems and networks (dsn),* 383 -392. doi: 10.1109/DSN.2010.5544294

Han, H., Sheng, B., Tan, C. C., Li, Q., & Lu, S. (2011). A timing-based scheme for rogue ap detection. *Parallel and Distributed Systems,* 11, 1912-1925. doi: 10.1109/TPDS.2011.125

Hou, H., Beyah, R., & Corbett, C. (2007, 26-30 Nov). A passive approach to rogue access point detection. *Global Telecommunications Conference,* 355-360. doi: 10.1109/GLOCOM.2007.73

Liu, C., & Yu, J. (2008, 8-13 June). Rogue access point based dos attacks against 802.11 wlans. *Fourth Advanced International Conference on Telecommunications*, 271-276. doi: 10.1109/AICT.2008.54

Ma, L., Teymorian, A., & Cheng, X. (2008, 13-18 April). A hybrid rogue access point protection framework for commodity Wi-Fi networks. *The 27th conference on computer communications*, 1220-1228. doi:10.1109/INFOCOM.2008.178

Schweitzer, D., Brown, W., & Boleng, J. (2007). Using visualization to locate rogue access points. *J. Comput. Small Coll.*, 23(1), 134-140. Retrieved from http://dl.acm.org/citation.cfm?id=1289280.1289310

Srilasak, S., Wongthavarawat, K., & Phonphoem, A. (2008, 24-26 April). Integrated wireless rogue access point detection and counterattack system. *Information security and assurance,* 326-331. doi: 10.1109/ISA.2008.103

Sriram, V., Sahoo, G., & Agrawal, K. (2010). Detecting and eliminating rogue access points in ieee802.11 wlan - a multi-agent sourcing methodology. *Second International Advance computing conference (IACC),* 256-260. doi:10.1109/IADCC.2010.5422999

Wei, W., Suh, K., Wang, B., Gu, Y., Kurose, J., & Towsley, D. (2007). Passive online rogue access point detection using sequential hypothesis testing with tcp ack-pairs. *The 7th ACM SIGCOMM conference on internet measurement* (pp. 365-378). New York, NY, USA: ACM. doi: http://doi.acm.org/10.1145/1298306.1298357