International Conference on Network Applications, Protocols and Services 2008 (NetApps2008)
21 - 22 November 2008
Executive Development Center, Universiti Utara Malaysia

Detecting Rogue Access Point (RAP) using Simple Network Management Protocol (SNMP)

Amran Ahmad, Suhaidi Hassan
College of Arts and Sciences
Universiti Utara Malaysia
{amran, suhaidi}@uum.edu.my

***Abstract*—Rogue access points (RAPs) expose the enterprise network to a barrage of security vulnerabilities in that they are typically connected to a network port behind the firewall. It will break any security implementation without a notice. Detecting RAP is vital to clear any threat to network environment. This paper is discussed about a method how to detect RAP such as passive monitoring, visualization and traffic analysis. We do a preliminary study using SNMP focusing on analyzing traffic analysis as a part of detecting RAP. We also propose a simple algorithm which is hope can detect RAP in advance before it vulnerable the network environment.**

***Index Terms*—Rogue Access Point (RAP), Simple Network Management Protocol (SNMP), SNMP Agent**

I. INTRODUCTION

Rogue access points (RAPs) expose the enterprise network to a barrage of security vulnerabilities in that they are typically connected to a network port behind the firewall [1]. Unauthorized or rogue access points (RAPs) produce security vulnerabilities in enterprise/campus networks by circumventing inherent security mechanisms [2][3] and installed on a secure network without the explicit permission of the appropriate network management authority [4]. The popularity of the 802.11-based Wireless LAN (WLAN) also increases its risk of security attacks such as Denial of Service (DoS) attacks [5]. This is happen due to open medium, insufficient software implementations, potential for hardware deficits, and improper configurations [2]. Even though APs are a best extensible device for network advancement, but it is also a main contributor to network vulnerabilities if its connect without proper security configuration [6].

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

The Simple Network Management Protocol (SNMP) forms part of the internet protocol suite as defined by the Internet Engineering Task Force (IETF) [7]. SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. It consists of a set of standards for network management, including an Application Layer protocol, a database schema, and a set of data objects. .

SNMP model consists of Network Management System (NMS), Manage devices and Management Information Base (MIB) [8]. NMS works as an interface (GUI) between network environment and Network Administrator. Any command or action taken is from NMS. Manage devices are device that can be managed by SNMP such as switch, router, gateway, computers or hardware related that have being supported by MIB. MIB provide a specific information of manage devices. Each device has its own MIB and provided from product manufacturer.

II. RELATED 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 open the service to any user. Detecting RAP is the first priority than denying it existent. Some related works have been done and can be categorized into three different categories:

A. Passive monitoring

The packet flowing for both wired and wireless have a different characteristics. It can be distinguish by using algorithm for computing Round Trip Time (RTT) [3]. 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 [9], consist of two different algorithm 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 algorithm 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.

B. 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. [4] 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.

C. Traffic characteristic

There are three kind of traffic characteristic [1]: 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 then 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 client 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.

III. SNMP at Works

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications. In typical SNMP usage, there are a number of systems to be managed, and one or more systems managing them. A software component called an agent runs on each managed system and reports information via SNMP to the managing systems.

Essentially, SNMP agents expose management data on the managed systems as variables (such as "free memory", "system name", "number of running processes", "default route"). The managing system can retrieve the information through the GET, GETNEXT and GETBULK protocol operations or the agent will send data without being asked using TRAP or INFORM protocol operations. Management systems can also send configuration updates or controlling requests through the SET protocol operation to actively manage a system. Configuration and control operations are used only when changes are needed to the network infrastructure. The monitoring operations are usually performed on a regular basis.

The variables accessible via SNMP are organized in hierarchies. These hierarchies, and other metadata (such as type and description of the variable), are described by Management Information Bases (MIBs).

A. SNMP basic components

An SNMP-managed network consists of three key components (see Figure 1):

- Managed device
- Agent
- Network-management systems (NMS)

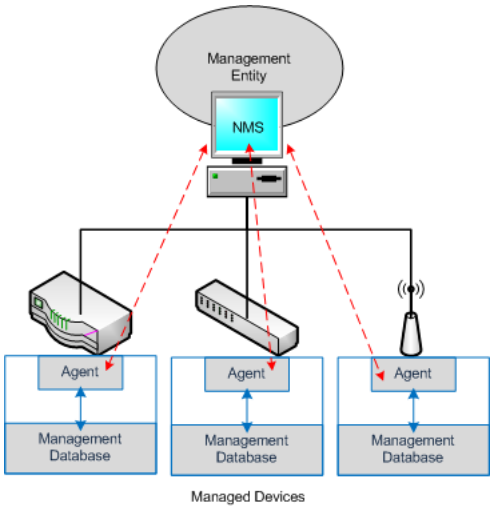

Figure 1. SNMP Basic Component

A managed device is a network node that contains an SNMP agent and that resides on a managed network. Managed devices collect and store management information and make this information available to NMSs using SNMP. Managed devices, sometimes called network elements, can be any type of device including, but not limited to, routers, access servers, switches, bridges, hubs, IP telephones, computer hosts, and printers.

An agent is a network-management software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP.

A network management system (NMS) executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network.

SNMP itself does not define which information (which variables) a managed system should offer. Rather, SNMP uses an extensible design, where the available information is defined by management information bases

(MIBs). MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing object identifiers (OID). Roughly speaking, each OID identifies a variable that can be read or set via SNMP. MIBs use the notation defined by ASN.1.

In telecommunications and computer networking, Abstract Syntax Notation One (ASN.1) is a standard and flexible notation that describes data structures for representing, encoding, transmitting, and decoding data. It provides a set of formal rules for describing the structure of objects that are independent of machine-specific encoding techniques and is a precise, formal notation that removes ambiguities.

ASN.1 is a joint ISO and ITU-T standard, originally defined in 1984 as part of CCITT X.409:1984. ASN.1 moved to its own standard, X.208, in 1988 due to wide applicability. The substantially revised 1995 version is covered by the X.680 series. An adapted subset of ASN.1, Structure of Management Information (SMI), is specified in SNMP to define sets of related MIB objects; these sets are termed MIB modules.

The MIB hierarchy can be depicted as a tree with a nameless root, the levels of which are assigned by different organizations. The top-level MIB OIDs belong to different standards organizations, while lower-level object IDs are allocated by associated organizations. This model permits management across all layers of the OSI reference model, extending into applications such as databases, email, and the Java EE reference model, as MIBs can be defined for all such area-specific information and operations.

A managed object (sometimes called a MIB object, an object, or a MIB) is one of any number of specific characteristics of a managed device. Managed objects comprise one or more object instances (identified by their OIDs), which are essentially variables.

IV. DETECTING RAP

In order to stop RAP the most capable aspect is how to detect it using SNMP. How SNMP can be used to detect RAP? (See Figure 2)

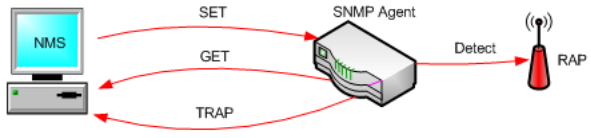

Figure 2. SNMP at work

NMS will SET agent into monitoring mode for detecting any new device attach to the nearest manage device. The agent will wait for PDU to arrive and trigger checking algorithm (traffic analysis). The algorithm will check either it is AP or other devices. If it is AP, agent will execute other algorithm which is specifically checking for either it is illegal AP or RAP. After RAP is found, SNMP agent will send TRAP to NMS for further action. NMS either automatically sends SET to block RAP or waiting for Network Admin to respond for any action. Another option is let agent does it automatically. Figure 3 shows the summary of flowchart used for detecting RAP.

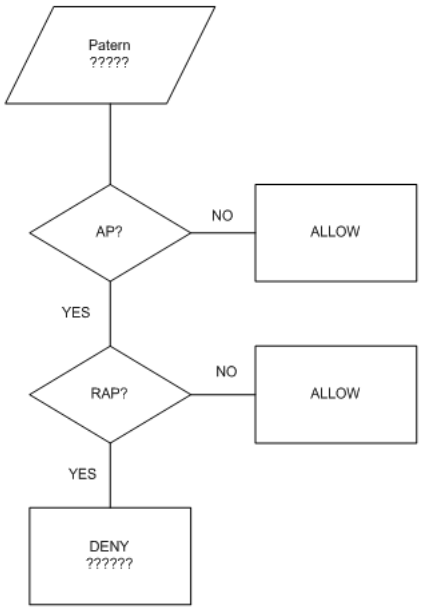

Figure 3. Detecting and Denying RAP Flowchart

So far there are no specific techniques how to detect RAP using SNMP for analyzing traffic analysis. As mentioned before there is only through identifying either one IP is attaching to MAC address (detecting non AP) or many IPs are attaching to MAC address (detecting AP). There are two choices how RAP can be identified; predefined allowed AP list or provide detection algorithm to agent which is not yet develop.

V. CONCLUSION

This paper has discussed on how to detect RAP using SNMP. Even though traffic analysis is better technique for discovering RAP, but further action should be taken to recognize RAP efficiently. We suggest by pre-define allowable AP list, the process will be more advance and detecting RAP is not difficult and consume more time without the list. However, it is not the only way to overcome the problem. Other technique such as passive monitoring and using visualization also promises for solving RAP detection problem.

REFERENCES

[1] R. Beyah, S. Kangude, G. Yu, B. Strickland, and J. Copeland, "Rogue access point detection using temporal traffic characteristics," *Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE*, vol. 4, pp. 2271–2275 Vol.4, 2004.

[2] L. Ma, A. Teymorian, and X. Cheng, "A hybrid rogue access point protection framework for commodity wi-fi networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, 13-18 April 2008, pp. 1220–1228.

[3] H. Hou, R. Beyah, and C. Corbett, "A passive approach to rogue access point detection," in *Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE*, 26-30 Nov. 2007, pp. 355–360.

[4] D. Schweitzer, W. Brown, and J. Boleng, "Using visualization to locate rogue access points," *J. Comput. Small Coll.*, vol. 23, no. 1, pp. 134–140, 2007.

[5] C. Liu and J. Yu, "Rogue access point based dos attacks against 802.11 wlans," in *Telecommunications, 2008. AICT '08. Fourth Advanced International Conference on*, 8-13 June 2008, pp. 271–276.

[6] S. Srilasak, K. Wongthavarawat, and A. Phonphoem, "Integrated wireless rogue access point detection and counterattack system," in *Information Security and Assurance, 2008. ISA 2008. International Conference on*, 24-26 April 2008, pp. 326–331.

[7] P. Drake, "Using snmp to manage networks," in *Designing Resilient Architectures, IEE Colloquium on*, 15 Nov 1991, pp. 2/1–2/4.

[8] Y.-S. Hwang and E. bae Kim, "An architecture of snmp-based network management of the broadband wireless access system," in *Communications, 2003. APCC 2003. The 9th Asia-Pacific Conference on*, vol. 3, 21-24 Sept. 2003, pp. 1163–1166Vol.3.

[9] W. Wei, K. Suh, B. Wang, Y. Gu, J. Kurose, and D. Towsley, "Passive online rogue access point detection using sequential hypothesis testing with tcp ack-pairs," in *IMC '07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*. New York, NY, USA: ACM, 2007, pp. 365–378.