NEW APPROACH IN WIRELESS INTRUSION DETECTION SYSTEM

Matej Kačic
Doctoral Degree Programme (1), FIT BUT
E-mail: xkacic00@stud.fit.vutbr.cz

Supervised by: Petr Hanáček
E-mail: hanacek@fit.vutbr.cz

Abstract: Today's wireless networks are vulnerable to eavesdropping, unauthorized access, denial of service attacks, etc. Wide usage of wireless networks cause concerns for these problems. This paper describes a concept of intrusion detection system for wireless networks. Proposed system is based on sensors, which sniff the data and send it to server, where analysis of these data is conducted. The analysis uses reputation system to rate wireless devices. The system will be able to detect already known or new kind of attacks.

Keywords: WIDS, WPA2, Wifi Security, Rogue Access Point, Wrap, Reputation systems

1 INTRODUCTION

Standard 802.11i [1] specifies wifi networks security protocols. It also describes security configurations RSN, popularly known as WPA2. It supports two types of authentication, Pre-shared key (PSK) and IEEE 802.1x. WPA2 uses AES for data encryption, but it also supports Temporal key integrity protocol (TKIP) used by old devices which are compliant to WEP (weak) encryption. On the other hand, AES stands for advanced encryption system and it is supported in current generation of Wifi devices. Standard WPA2 is considered to be "safe" in wifi community.

This paper describes two main problems of wifi network and detection and/or prevention from those vulnerabilities. In last chapter a new concept of Wireless Intrusion Detection system based on reputation system will be introduced. The main motivation to design this system is detection of well-known attacks, detection of any new form of attacks and detection of authorized users' malicious behavior.

2 WIFI SECURITY PROBLEMS

Two main problems of wifi networks security, new vulnerability Hole 196 and problem of Rogue access point, are described in this section.

2.1 HOLE 196

In the past, several attacks were published on WPA/WPA2 authentication and encryption. For example, WPA authentication mode Pre-shared key (PSK) is vulnerable to eavesdropping a dictionary attack[2] or temporal key integrity protocol (TKIP) vulnerability allows attacker to guess IP address of the subnet and then inject few small size frames to cause disruption in the network[2]. Conference Defcon 18 in summer 2010 brings new vulnerability of WPA2 enterprise encryption called "hole 196" [4]. Its name is derived from the fact that the vulnerability was discovered on page 196 of the 802.11 IEEE standard. It allows a malicious insider (authorized user) to spoof the MAC address of the access point and to inject a GTK encrypted packet with broadcast destination address. The insider is able to launch several attacks such as ARP poisoning. ARP poisoning is a classic attack that could already

be launched on Ethernet or WPA2 secured AP. In this old way of attacking AP forwards all spoofed packets on wireless and wired networks.

Usually, wired networks provide systems such as IDS/IPS, which can rapidly catch and block this attack. On the other hand, launching ARP poisoning attack using spoofed GTK encrypted frames limits the areas of the attack only to air. Figure 1 compares those two types of ARP poisoning attack. It is obvious that this vulnerability enables to launch this attack, while intruders stay hidden.

The "hole 196" allows to launch several other attacks. First, target attack can be used to malware injection, DNS manipulation, Port scanning of wifi client with IP address corresponding with destination IP present in the attacker's packet. All other wifi clients reject the packet. GTK vulnerability can also be exploited to launch DoS attack in Wireless networks.

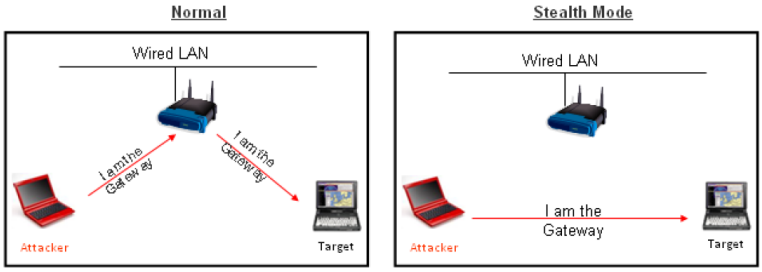

Figure 1: Normal vs Stealth mode ARP poisoning [4].

We have several options to protect wifi networks against the "hole 196" vulnerability. Client side IDS can detect ARP cache poisoning or any malware injection. However, there is a limitation to use this kind of software by varieties of client devices such as smartphone, ipad and so on. Client isolation technique is only first-aid solution and could be bypassed by another variant of the ARP poisoning. [5]

Nowadays, we can use a Wireless intrusion detection/prevention system to protect wifi network not only against well-known attacks including "hole 196" like attacks but also against new attacks. This article in last section describes a new concept of wireless intrusion prevention system.

2.2 Rouge Access Point

Many organizations use Wifi to provide access to internet or their workspace. Wifi provides more flexible environment than wired network, but everyone within range of the wireless signal can easily catch data. Most enterprise wifi access points include the highest security mechanism today, WPA2 based on AES cipher. This mechanism protects user from data eavesdrop and unauthorized access. On the other hand, no security measures can protect your data from unauthorized installation of access points. The staffs or intruders usually create rogue access point by plugging in AP to wire network. This act causes many security threats, for example hacker can bypass all network defenses (firewall, access control).

So, we can define rouge AP as AP that is installed to network without authorization and does not follow security policy or as AP that has setup based on the malicious intention to compromise the organization's information system i.e. data sniffing[11].

There are four types of rouge AP. First, Employee's rouge access point, which is installed on the organization's LAN without authorization. Next type is Attacker's external AP which is setup outside the company and it does not connect to LAN. Third type, Attacker's internal AP, creates a backdoor to company's LAN. And the last type is Neighborhood rouge AP where this AP is setup by other

company.

Detection of rouge AP can be done only by collecting wireless data, including Beacon and Probe frames and after that the system evaluates the sniffing data. Wireless intrusion system provides this feature.

2.3 RELATED WORKS

There are several products that provide IDS capability for wireless networks. Motorola AirDefence[6] services platform identifies any rouge device by analyzing networks traffic and determine the level of threat that potential rouge poses to an organization. It uses a distributed architecture of remote sensors and centralized server appliance to constantly monitor all wireless activity constantly in real time allowing enterprises to control the wireless air space and define and enforce policy compliance.

AirMagnet[7] has ability to provide Wi-Fi security policy management, wireless intrusion detection, rogue access point detection, connection troubleshooting, trend analysis, reporting and capacity planning and may even assist in the site survey process. Airtightnetworks[5] has patented a classification techniques identifying those connections that pose a genuine risk to your security.

One of open source wireless IDS is Kismet[9] providing a stateless and stateful IDS for layer 2 and layer 3 wireless attacks. Kismet can alert on fingerprints (specific single-packet attacks) and trends (unusual probes, disassociation floods, etc).

WiFi Miner[10] solution approach is to find frequent and infrequent patterns on pre-processed wireless connection records using infrequent pattern finding Apriori algorithm. An anomaly score is assigned to each packet based on whether the record has more frequent or infrequent patterns. Connection records with positive anomaly scores have more infrequent patterns than frequent patterns and are considered for anomalous packets.

3 NEW DESIGN OF WIRELESS IDS

The following section deals with new design of wireless intrusion detection system. Base blocks of function are introduced in next part.

3.1 FUNCTIONAL CONCEPT

Our wireless intrusion detection system consists of wifi node, switch and server. Wifi nodes have to be placed in area we can protect from intruders and they capture all necessary wifi communication. Nodes are connected with server via wired Ethernet using switch and send captured wifi communication to server constantly. Figure 2 shows in detail a functional schema of this concept.

At first, server provides a preprocessing of incoming data to extract all necessary attributes. After that those attributes are stored in database and an analysis can be started. Analyzing packets based on reputation system are described in detail in section 3.4. System tries to identify malicious behavior in secured area. It also does some action to slow intruders or even to stop them.

Important feature today is localization of wifi station or access point in secured area. We can divide wifi devices to two categories, access point devices and mobile devices. Procedure of localization will be different depending on those categories. Access point devices are connected to company's LAN infrastructure and we can easily find out port where device is connected. Mobile device is associated with some access point and it is situated in range of one or more wifi nodes. Intersection of information from wifi node and possibly information from access point is possible to guess approximate position of device. This feature can also be computed on server.

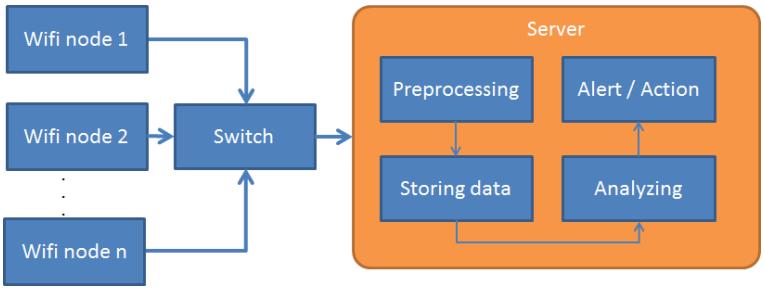

Figure 2: Schema of wireless intrusion system.

3.2 HARDWARE EQUIPMENT

As Wifi node uses WRAP single board computer optimized for wireless access and network routing application from PCEngines. This board has one i386 platform processor at 266MHz, 64 MB SDRAM, Compact Flash reader, serial port and two miniPCI slots, which are used by wireless card CM9 based on chipset Atheros AR5213. CM9 supports wifi standard IEEE 802.11a/b/g and all necessary security mechanisms such as WEP, WPA, WPA2. It also supports different operation modes like managed, monitor and access point mode. The whole unit is placed to metal box with two antennas connected to CM9.

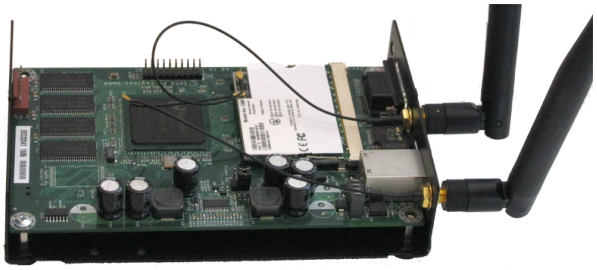

Figure 3: Wrap single board with CM9 card and two antennas.

3.3 SOFTWARE EQUIPMENT

On every wifi node the operating system FreeBSD 8.2 is installed. It was necessary to make some changes in FreeBSD kernel and configuration. WRAP is an embedded system, that's why the Compactflash disk has to be in read only mode. All configuration's files are stored in separated partition. While booting the system this partition is mounted and every configuration file is mirrored to system configuration directory and partition is immediately unmounted. Although WRAP board is embedded system and is designed for specific operating system with limited features, our modified FreeBSD provides full features of this operating system.

Aircrack-ng [3] is a set of tools for auditing wireless networks and was successfully installed on WRAP. It includes tool named Airserv-ng which is a wireless card server allowing multiple wireless application programs to use a wireless card independently via client-server TCP network connection. We can run Airserv on each wifi node which allows us to send captured packets to server easily. On server side we use another tool Airdump to store packets for analysis.

3.4 ANALYZE BASED ON REPUTATION SYSTEM

Every user of wifi device has different behavior or needs. Not always is his behavior safe or allowed. The idea is to use a reputation system and rate different wifi clients based upon their reputation. This is based on using a system of cataloging, which looks at the profile of client behavior on the wifi networks, categorizing the reputation of the devices and then deciding whether a device or wifi user is risky or not. This approach will be able to recognize a malicious or suspicious behavior of authorized and unauthorized devices and also detect new potential form of attacks.

4 CONCLUSION

In this paper a new approach of wifi protection was proposed, the wireless intrusion detection system based on reputation system with suspicious and malicious behavior detection of wireless devices. Currently Wrap platform with operating system FreeBSD 8.2 is fully functional which means that the captured data are successfully sent to server. This approach is only a concept and there is a lot of future work. It is necessary to design profiles of client behavior, reputation model and calculation of score for rating wireless clients. An important step in research is choosing the right entry data for analysis. I believe this concept will contribute to improve wireless network security.

ACKNOWLEDGEMENT

The research has been supported by the Czech Ministry of Education in frame of the Research Intention MSM 0021630528: Security-Oriented Research in Information Technology, MSM 0021630503

REFERENCES

[1] *IEEE Std 802.11i-2004.* USA : IEEE, 2004. 190 s. ISBN 0-7381-4074-0.

[2] Beck, M., Tews, E.: *Practical attacks against WEP and WPA* [online]. 2010 [cit. 2011-03-03]. WWW: <http://dl.aircrack-ng.org/breakingwepandwpa.pdf>

[3] *Aircrack-ng* [online]. 2010 [cit. 2011-03-03]. WWW: <http://www.aircrack-ng.org/>.

[4] AHMAD, Md. WPA Too!. In *DEFCON-18* [online]. Las Vegas, 2010 [cit. 2011-03-03]. WWW: <http://www.defcon.org/images/defcon-18/dc-18-presentations/Ahmad/DEFCON-18-Ahmad-WPA-Too-WP.pdf>.

[5] AirTight Networks: WPA2 Hole196 Vulnerability: Exploits and Remediation Strategies, 2010 [cit. 2011-03-03]. WWW: <http://www.defcon.org/>

[6] *Airdefence* [online]. 2010 [cit. 2011-03-03]. WWW: <http://www.airdefense.net/>.

[7] *AirMagnet* [online]. 2010 [cit. 2011-03-03]. WWW: <http://www.airmagnet.com/>.

[8] *Airtight* [online]. 2010 [cit. 2011-03-03]. WWW: <http://www.airtightnetworks.com/home/solutions /wireless-intrusion-prevention.html/>.

[9] *Kismet* [online]. 2010 [cit. 2011-03-03]. WWW: <http://www.kismetwireless.net/>.

[10] Rahman, A.,Ezeife, C., Aggarwal, A.: WiFi Miner: An Online Apriori-Infrequent Based Wireless Intrusion System, In: Knowledge Discovery from Sensor Data, Springer Berlin / Heidelberg, 2010, p. 76-93

[11] Songrit, S.,Kitti W.,Anan P.: Integrated Wireless Rogue Access Point Detection and Counterattack System, IEEE Computer Society, pp. 326-331, Apr. , doi:10.1109/ISA.2008.103