Anomaly Based Wi-Fi Intrusion Detection System

Pratik Satam

(Supervised by Dr Salim Hariri)
NSF Cloud and Autonomic Computing Center, The University of Arizona,
nsfcac.arizona.edu
pratiksatam@email.arizona.edu

Abstract— **The omnipresence of mobile devices and the great need to remain connected has brought to the forefront, the ever-growing need for wireless networks. This unprecedented growth of wireless networks and their use has resulted in an era where, the security of wireless networks has become a necessity. Currently the security methods to protect the Wi-Fi are based on the use of cryptography techniques to protect the data. But these methods fail to address the issue of availability of the service (against DOS), or Integrity (against Mac address spoofing).**

As a part of this Ph.D research, I present two architectures to develop an anomaly based intrusion detection system for single access point and distributed Wi-Fi networks. These architectures can detect attacks on Wi-Fi networks, classify the attacks and track the location of the attacker once the attack has been detected. The system uses statistical and probability techniques associated with temporal wireless protocol transitions, that we refer to as Wireless Flows (Wflows). The Wflows are modeled and stored as a sequence of n-grams within a given period of time. We studied two approaches to track the location of the attacker. In the first approach, we use a clustering approach to generate power maps that can be used to track the location of the user accessing the Wi-Fi network. In the second approach, we use classification algorithms to track the location of the user from a Central Controller Unit. Experimental results show that the attack detection and classification algorithms generate no false positives and no false negatives even when the Wi-Fi network has high frame drop rates. The Clustering approach for location tracking was found to perform highly accurate in static environments (81% accuracy) but the performance rapidly deteriorates with the changes in the environment. While the classification algorithm to track the location of the user at the Central Controller/RADIUS server was seen to perform with lesser accuracy then the clustering approach(76% accuracy) but the system's ability to track the location of the user deteriorated less rapidly with changes in the operating environment.

Keywords: — Anomaly detection, IEEE 802.11 security, Intrusion detection, Network security, Protocol analysis, Wireless networks.

I. MOTIVATION

The IEEE protocol 802.11 is a wireless local area network (WLAN) protocol first formalized in the year 1997 [1]. This protocol has experienced numerous security improvements since its inception. The protocol when initially introduced used Wired equivalent protection (WEP) encryption scheme. Wi-Fi Protected Access (WPA) later introduced in the 802.11i [2] in 2004. The WEP protocol that was initially used for secured communication over the Wi-Fi had cryptographic weaknesses and could be cracked easily when the attacker had enough sample traffic[3]. The subsequent modifications to the protocol have brought to the forefront better cryptographic schemes that ensure the security of the data frames passed over the network. But the network remains vulnerable to attacks on the data link layer which by protocol design must go unencrypted. Thus, leaving the network susceptible to denial of service (DoS) attacks and attacks that result from packet forgery [4].

To facilitate, better network access, companies and institutions have deployed distributed Wi-Fi networks. These distributed networks use pre-authentication to the access points as a means of allowing the users to access the wireless network over large areas, where the user is seamlessly able to stay connected as he/she moves around the facility by using different access points, but these distributed Wi-Fi networks are still susceptible to denial of service attacks (DoS) and packet forgery attacks. Moreover, once an attack has been detected it's important that we obtain the location of the attacker to prevent any further attacks.

II. OBJECTIVE

The main research objectives are twofold 1) Development of an anomaly based intrusion detection system for single access point and distributed Wi-Fi networks, that is highly accurate in detection, can detect new and zero day attacks and has low false positives and no false negatives; and 2) Development of a tracking system that is able to track the location of the actual user and is able to separate the location of the attacker from the normal users using machine learning approach.

The proposed approach will result in the development of online runtime monitoring modules that will monitor illegal exploitations of existing vulnerabilities in the IEEE 802.11 protocol and use the rules obtained during the machine learning stage to detect an attack, classify the attack and then detect the location of the attacker.

978-1-5090-6558-5/17 $31.00 © 2017 IEEE
DOI 10.1109/FAS-W.2017.180

III. METHODOLOGY

Figure 1 shows the general architecture of the system [5] that is deployed in each of the access points that make up the distributed Wi-Fi network. The main modules are of the system in the access points are: 1) Sniffer that collects Wi-Fi frames, 2) Behavior Authentication Module that generates the n-grams, Wflows [5] and perform behavior analysis to detect and classify Wi-Fi attacks, and 3) Location tracking module that helps the access point to judge the distance of the user from the access point.

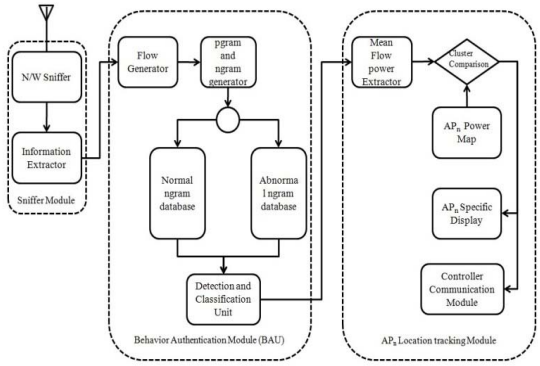

Figure 1. IEEE 802.11 Behavior Analysis module and Tracking module architecture for AP_n.

Figure 2 shows the architecture of the Central Controller for the network [5] which performs the task of combining the location information from different access points to determine the final location of the attacker.

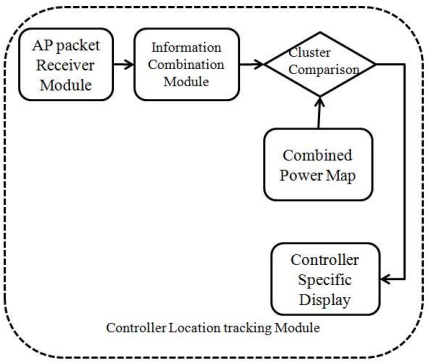

Figure 2. Central Controller Architecture.

The system operates in two main phases: Training phase where we model the normal and abnormal behavior of the Wi-Fi frames for the Behavior Authentication Module. During the training phase, we also perform the Area Power mapping for each of the access points for the Location tracking module in each of the access points. The second phase is the Detection phase that is used to detect and identify the locations used to launch WiFi attacks.

IV. RESEARCH PLAN

Our research plan is to enhance the performance and scalability of the WiFi IDS algorithms. The current WiFi location accuracy is at 81 % and our goal is to improve it up to uppoer 90%. Our current algorithms showed an acceptable performance level to detect known attacks (eg. De-Authentication attack, Injection Test, Association Flood). Our research plan is to improve on these algorithms such that they can also detect modified attacks or new ones, can classify the attacks being launched, and then identify the attack locations. The future work will also investigate techniques to make our WiFi IDS algorithms resilient to attacks and any changes in the operational environments.

REFERENCES

[1] IEEE Std 802.11-1997 Information Technology- telecommunications And Information exchange Between Systems-Local And Metropolitan Area Networks-specific Requirements-part 11: Wireless Lan Medium Access Control (MAC) And Physical Layer (PHY) Specifications. 1997.

[2] [2] Institute of Electrical and Electronics Engineering, 2004. IEEE802.11i-2004: Amendment 6: Medium Access Control (MAC)Security Enhancements. IEEE Standards. 2004-07-23.

[3] [3] S. Fluhrer, I. Mantin and A. Shamir, Weaknesses in the Key Scheduling Algorithm of RC4. Selected areas in cryptography, 2001 – Springer (2001).

[4] [4] A. Lashkari, M. Danesh and B. Samadi, “A survey on wireless security protocols (WEP, WPA and WPA2/802.11i)”, Computer Science and Information Technology, Beijing, pp 48- 52, August 2009.

[5] Satam, Pratik. "An Anomaly Behavior Analysis Intrusion Detection System for Wireless Networks." (2015).