

Substantiating Unexpected Behavior of 802.11 Network Hosts

Elankayer Sithirasenan and Vallipuram Muthukumarasamy
Institute for Integrated and Intelligent Systems
Griffith University, Gold Coast Campus, Australia
{e.sithirasenan, v.muthu}@griffith.edu.au

Abstract

With the increasing dependence on wireless LANs (WLANs), businesses and educational institutions are in desperate need of a robust security mechanism. The latest WLAN security protocol, the IEEE 802.11i introduces Robust Security Networks (RSN) and assures rigid security for wireless environments with the support of IEEE 802.1x protocol for authentication, authorization and key distribution. Nevertheless, users remain skeptical since they lack confidence on the trustworthiness of these security mechanisms. In this paper we investigate and test a novel Early Warning System (EWS), built on the foundations of IEEE 802.11i security architecture. Our system is developed to detect anomalies and prevent intrusions in real-time. It has several levels of defense to protect the wireless hosts from a range of security threats. Security alerts are raised only when the legitimacy of abnormal conditions is validated using effective outlier based data association techniques.

1. Introduction

During the last decade, significant research work has been carried out on improving the intrusion detection systems (IDS), mainly in wired networks. For wireless networks, the issues are even more challenging. Ever increasing security threats and the dynamic nature of wireless network usage demand more reliable and fast intrusion detection or prevention techniques. Unfortunately, many organizations find it difficult to use even the available techniques effectively, mainly because of the complexity of deployment, lack of information about its appropriate use and the amount of false positives. Our WiFi-EWS helps network security administrators, integrators and end-users to confidently utilize their wireless networks to meet the expectations of their organization.

The wireless network environment is exposed to a range of intrusion attacks. The most common is “War-driving” using a laptop and a War-driving software such as NetStumbler. The attack generally exploits the famous weakness in Wired Equivalent Privacy (WEP) encryption used by IEEE 802.11b networks [4, 5]. This is usually a second stage following the detection of a secured AP by War-driving. The most commonly used tool for WEP key extraction is the Linux program AirSnort [3]. AirSnort is a passive monitor and does not throw any messages out. Session hijacking combines denial-of-service (DoS) and identity spoofing attacks. Typically an attacker forces a legitimate station (STA) to terminate its connection with an access point (AP) by sending a disassociation/deauthentication frame with the source MAC address spoofed to be that of the AP. This results to the STA disconnecting from the network and enabling the adversary to associate with the AP by masquerading the MAC address of the STA, hence taking control of its session.

The wireless threats discussed above are some of the common ones. Although the new security architecture guarantees robust security, the chances of emerging new threats are inevitable. Hence, the aim of our WiFi-EWS is to effectively protect the wireless environment from any known or new threats. In this respect our WiFi-EWS is developed adopting a two-phased approach specifically for wireless networks employing IEEE 802.11i security architecture [8]. WiFi-EWS combines anomaly-based methods together with outlier based data association techniques for preventing intrusions and/or to detect them in advance. The main features of our approach are: 1. use of adaptive learning mechanism to keep track of various round trip timings of management frames, 2. the use of event profiles to track the behavior of all participating hosts and to detect abnormal behavior, 3. accumulating historical data and querying them on-the-fly enabling fast detection of outliers in large databases to quickly vali-

date abnormal conditions.

To verify the legitimacy of abnormal events the WiFi-EWS builds a repository of captured events on a Beowulf cluster as a partial data cube. It focuses on establishing the legitimacy of illegitimate events by analyzing it from different view points. The use of data cubes in the parallel footing makes it viable. Our system is novel and effective with the ability of detecting outliers in real time enabling lesser number of false positives/negatives.

This paper is organized as follows. In Section 2 we give an overview of related work on anomaly detection and currently available products. Section 3 briefly illustrates the concept behind the WiFi-EWS. Details of experiments carried out to verify the effectiveness of our approach are discussed in Section 4. Results and analysis are given in Section 5. Section 6 concludes the paper.

2. Related Work

There exists a number of well established IDSs for wired networks. Experiences from such systems could help in the wireless environment. In this respect we take a quick look at host and network based IDSs.

The host based IDS proposed by Ilgun et al. [9] focuses on state transition analysis of computer penetrations. It uses an audit record independent rule-base that is easier to read than the audit record dependent penetration rule bases. It also provides greater flexibility in identifying variations of known penetrations. State transition analysis also provides a modest, but intuitive procedure for rule generation, rather than ad-hoc approaches that are currently in use. Vigna et al. [14] extended the above work and developed a tool for Network-based Intrusion Detection - NetSTAT aimed at real-time network-based intrusion detection. It extends the state transition analysis technique to network based intrusion detection in order to represent attack scenarios in a networked environment. NetSTAT is oriented towards the detection of attacks in complex networks composed of several subnets.

Paxson's [11] stand-alone system "Bro" observes network traffic directly and passively, using a packet filter. The system is conceptually divided into an "event engine" that reduces a stream of (filtered) packets to a stream of higher-level network events, and an interpreter for a specialized language is used to express the site's security policy. The events are compared with the security policy for anomalies.

In addition to intrusions, the wireless networks face additional security issues mainly due to the inherent qualities of the communication medium. Security is-

issues such as session hijack and network injection are more common in wireless networks because of the exposed channels. Although, considerable work has been reported addressing these issues, the possibility of such vulnerabilities on the new security architecture is yet to be explored. In this view, our aim is to detect security issues that could arise during the 802.1x mutual authentication process. Since we are using anomaly based techniques for this purpose, we investigate similar systems.

Hall et al. [7] introduced anomaly based intrusion detection using mobility profiles. They suggested enhancing their system by supplementing existing user and device-based profiles, with those based on mobility. This system is more suitable for addressing the problem of stolen cell phones, given that the mobility behavior of the thief and the user are likely to be different. In the case of wireless networks the attacker needs to be in the same vicinity as the user to carry out an attack. Therefore the use of mobility profiles will not be suitable for wireless networks. Lim et al. [10] introduced a low cost solution for intrusion detection and response. Their system detects intrusions by various means such as MAC address filtering, tracking RTS/CTS to detect passive intruders and stateful monitoring to detect random responses by intruders. The prototype developed had several limitations in the processing power, hence the authors focused only on selected intrusions. They mainly considered DoS attacks and their system detected the NetStumbler without any false positives.

Gill et al. [6] proposed a passive technique for detecting session hijacking attacks. They use Received Signal Strength (RSS) and Round Trip Timings (RTT) to detect anomalies. Both cases require frequent re-tuning of threshold values for satisfactory performance. However, their system cannot be extended to detect other security threats in the wireless environment.

In addition to the above techniques there are several commercial products used for intrusion detection and preventions. AirDefence [1] and Air Magnet [2] claim to provide a complete hardware and software solution for intrusion detection and prevention in 802.11 wireless networks. AirDefence detects intruders and attacks and also analyzes vulnerabilities. Although the manufacturers claim their system provides active responses to every possible intrusion attempts there is no statistical evidence to justify it. Furthermore, WLANs with 802.1x authentication are yet to become popular and hence the credibility of the commercial systems still needs to be verified.

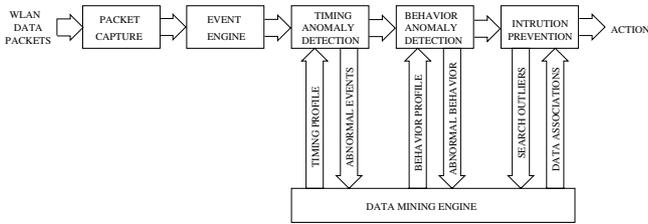


Figure 1. WiFi-EWS Block Diagram

3. Proposed WiFi-EWS

Figure 1 illustrates the conceptual block diagram of our proposed WiFi-EWS. It includes a packet capturing module, an event engine, a timing anomaly detection module, a behavioral anomaly detection module, an intrusion prevention module and the data mining engine. The data mining engine is one of the main components in our system with the ability of processing outlier based data association requests efficiently, preventing intrusions in real time. Our WiFi-EWS has several levels of defense offering improved reliability for anomaly detection. The first level of defense is the discovery of timing anomalies followed by the discovery of behavioral anomalies. If an event is discovered with either or both anomalies a third level of defense is set off to validate the legitimacy of the anomaly based on historical data. Since the WiFi-EWS needs to search enormous amounts of historical data in real time we use parallel processing techniques to search our data base. A detailed description of our proposed system can be found in [12].

4. Experiments

Our experimental setup consists of a small Beowulf cluster, 802.1x enabled Access Points (APs) and a few clients configured to communicate with the 802.1x enabled access points. The Beowulf cluster has three nodes including the head node. The head node is a Pentium 4 machine with 1GB internal memory and 120GB secondary storage. The nodes are all Pentium III machines with 256MB internal memory and 40GB secondary storage. The head node is also configured to capture the wireless network traffic in promiscuous mode and deliver it to the relevant modules for further analysis. One of the nodes in the cluster runs the RADIUS server software and acts as the authentication server for the access points.

Let us now look at each modules in our system with practical examples. First, to detect timing anomalies the WiFi-EWS maintains a timing profile for every par-

Request/Response	Max	Min
Open Auth	0.97	0.35
Open Assn	6.24	0.54
EAP Ident	2.63	0.04
EAP PEAP	4.31	0.08
TLS Client Hello	10.36	0.09
EAP TLS	9.39	0.08
TLS Server Hello	28.87	27.02
TLS Certificate	10.71	0.08
TLS Change Cipher	4.16	0.08
EAP Key	26.36	7.70
Overall	244.62	189.56

Table 1. EAP-TLS Timing Profile

Request/Response	Time
Open Auth	0.36
Open Assn	0.55
EAP Ident	1.12
EAP PEAP	0.80
TLS Client Hello	101.14
EAP TLS	283.09
TLS Server Hello	665.78
TLS Certificate	259.81
TLS Change Cipher	1.66
EAP Key	8.71
Overall	1424.35

Table 2. EAP-TLS Abnormal Timing

ticipating host in the wireless environment. Typical example values are shown in Table 1. Maximum and Minimum timings are used for identifying timing anomalies during message transfers. A timing anomaly is raised when a host exhibits an abnormal timing value during a round trip message transfer, i.e. the time taken to send a message and to receive the respective response.

The timing values shown in Table 2 were obtained during a typical DoS attack. Here neither the access point nor the station was targeted. However we injected several Deauthentication frames with a bogus MAC address jamming the media. During this period we initiated an authentication process and the timings were noted. From the timings it is obvious that the values shown for the challenge/exchange process was extraordinarily high resulting in the high overall timing. Thus we could detect that the hosts are experiencing an abnormal condition. Although the DoS attack did not affect the authentication process itself the timing anomaly detection module will show only a time delay in the authentication process. To further investigate the legitimacy of this anomaly we pass this information to the third phase - the intrusion prevention module.

The second level of defense in WiFi-EWS is the behavioral anomaly detection. In order to ascertain the behavior of the participating hosts we used the RSN projection model developed in [13]. The first stage in behavioral analysis is to compare the current behavior with that of the normal behavior of the respec-

802.11 Authentication
802.11 Authentication
802.11 Association Request
802.11 Association Response
EAP Request Identity 1
EAP Response Identity 1
EAP Request PEAP 2
EAP Response NAK 2
EAP Request TLS 3
EAP Response TLS 3
EAP Request TLS 4
EAP Response TLS 4
EAP Request TLS 5
EAP Response TLS 5
EAP Request TLS 6
EAP Response TLS 6
EAP Request TLS 7
EAP Response TLS 7
EAP Success 7
EAPOL Key
EAPOL Key
EAPOL Key
EAPOL Key

Table 3. EAP-TLS Authentication Behavior

802.11 Deauthentication
802.11 Probe Response
802.11 Probe Response
802.11 Authentication
802.11 Authentication
802.11 Association Request
802.11 Association Response
EAPOL Key
EAPOL Key
EAPOL Key
EAPOL Key
802.11 Null function (No data)
802.11 Null function (No data)

Table 4. Behavior During A Replay Attack

tive hosts. Typical normal behavior for a EAP-TLS authentication process is shown in Table 3. A normally behaving host traverses all the legitimate behavior as in the RSN projection model. If anomalies occur there can be situations where hosts fall into illegitimate states and do not match the projection model. Table 4 shows the typical packets captured during a replay attack carried out by a legitimate station. In this scenario the 4-way handshake takes place straightaway since the station is already in possession of the PMK. Although this type of attack is not of much interest in RSN, it is a possible behavior if the PMK is compromised. However, WiFi-EWS does not instantly consider such anomalies as illegitimate, but they track such events and forward it to the intrusion prevention module for validation.

The third level of defense is one of the most important features in the WiFi-EWS and the module that executes this defense is called the intrusion prevention module. This module derives important decisions to verify the significance of the anomalies discovered by the previous modules. Hence this module plays an important role in maintaining the reliability and depend-

STA	Event	Freq	STA	Event	Freq
12	27	8676	14	27	764
12	42	110563	14	42	2478
12	76	7431	14	76	657
12	195	53	14	195	32
12	229	72	14	229	50
12	245	34	14	245	39
12	257	23	14	257	24
12	281	77	14	281	62
12	339	115	14	339	542
12	343	6231	14	343	128
12	348	130	14	348	6939

Table 5. DoS Attack - Query Results

ability of our system. In order to achieve our main goal of real time intrusion prevention, we have adopted an efficient querying technique to search our data cube for outlier based data associations. Preliminary results obtained from the outlier detection process are discussed in the next section.

5. Results and Discussion

The intrusion prevention module executes a number of data association requests to decide whether anomalies detected by the two anomaly modules are significant or not. Table 5 shows a typical data association between stations and events. These associations were extracted from the data cube with a single query. Using this data association we can investigate all events associated with the stations. In this table, column “STA” shows the station ID and column “Event” shows the event ID. The numerical values in the “Freq” column gives the frequency count for each associations. Using the data cube we can obtain similar associations from different data views in real time with a single query. Such associations form the basis of substantiating unexpected behavior in our system. For example in Table 5 station 12 exhibits extraordinarily high frequency for event 42 - Deauthentication. The timing anomaly shown in Table 2 was due to this high number of deauthentication requests. Thus, the timing anomaly could be validated using the data associations if we find an association with significant extremeness or remoteness (a support value greater than a upper threshold value or less than a lower threshold value set by the training algorithm). Such extreme or remote conditions are considered as anomalies. On the other hand if an anomaly does not meet the required threshold we ignore it and update the profiles of the station to reflect the conditions.

In order to verify the behavioral anomalies observed during the replay attack we queried the data cube on different views. We queried for events necessary to identify the effect of the replay attack. Hence, we used

Source ID	Destination ID	Event ID	Count
12	0	76	11891
14	0	76	664
0	12	95	974
0	14	95	276
0	12	323	64
0	14	323	282

Table 6. Replay Attack - Query Results

only those events related to the authentication process. In an IEEE 802.11i/WPA2 environment a station requests to associate with an access point giving its credentials. The access point will respond favorably if it agrees with the security credentials advertised by the station. Therefore, we obtained query results for AssociationRequest (76), AssociationResponse (95) and EAPSuccess (323) events. Table 6 shows the typical results obtained from these queries on our experimental setup. The first block shows the number of AssociationRequest events for station 12 and station 14 respectively. The second block shows the number of AssociationResponse events for station 12 and station 14 respectively. The third block gives the number of EAP Success events for the two stations. These results indicate some abnormality with station 12. Station 14 has almost equal number of EAP Success events corresponding to the number of AssociationResponse messages sent by Access Point (0). Therefore, if we scale the data associations for station 12 on its EAP Success event in relation to rest of the stations in the environment we can discover whether station 12 is facing any behavioral anomaly or not.

6. Conclusion

In this paper, we have investigated and tested a novel intrusion prevention technique for WiFi Networks based on efficient outlier based data association techniques. The proposed method is based on combining anomaly based intrusion detection with outlier based data associations. The initial experimental results obtained with the RSN environment are promising and confirming the concept of the proposed system. The proposed system has the ability to detect anomalies in real time without apriori knowledge.

In the future work, the WiFi-EWS will be fully implemented in large scale and the performance of the complete system will be tested. Although this technique is expected to provide promising results in cooperate networks, their applicability to smaller networks may be limited due to resource requirements.

References

- [1] AirDefence - intrusion protection and monitoring. <http://www.airdefense.net/products/enterprise.php>. Cited March 2006.
- [2] AirMagnet - wireless network management systems. <http://www.airmagnet.com/products/enterprise.htm>. Cited March 2006.
- [3] AirSnort - WLAN tool which recovers encryption keys. <http://airsnort.shmoo.com>. Cited March 2006.
- [4] N. Borisov, I. Goldberg, and D. Wagner. Intercepting mobile communications: The insecurity of 802.11. In *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, pages 66–72, Rome, Italy, July 2001.
- [5] S. Fluhrer, I. Mantin, and A. Shamir. Weaknesses in the key scheduling algorithm of RC4. *Lecture Notes in Computer Science*, 2259:1–24, 2001.
- [6] R. Gill, J. Smith, M. Looi, and A. Clark. Passive technique for detecting session hijacking attacks in ieee 802.11 wireless networks. In *AusCERT '05: Proceedings of the 4th Asia Pacific Information Technology Security Conference*, pages 26–38, May 2005.
- [7] J. Hall, M. Barbeau, and E. Kranakis. Anomaly-based intrusion detection using mobility profiles of public transportation users. In *Proceedings of the IEEE International Conference on Wireless And Mobile Computing, Networking And Communications*, volume 2, pages 17–24, August 2005.
- [8] IEEE Standard 802.11i Part 11. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Medium Access Control (MAC) Security Enhancements*, July 2004.
- [9] K. Ilgun, R. Kemmerer, and P. Porras. State transition analysis: A rule-based intrusion detection approach. *IEEE Transactions on Software Engineering*, 21(3):181–199, January 1995.
- [10] Y. Lim, T. Schmoeyer, J. Levine, and H. Owen. Wireless intrusion detection and response. In *Proceedings of the IEEE Systems, Man and Cybernetics Society Information Assurance Workshop*, volume 18, pages 68–75, June 2003.
- [11] V. Paxson. Bro: a system for detecting network intruders in real-time. *Computer Networks (Amsterdam, Netherlands: 1999)*, 31(23–24):2435–2463, 1999.
- [12] E. Sithirasenan and V. Muthukumarasamy. An Early Warning System for IEEE 802.11i Wireless Networks. In *AusWireless'06: Proceedings the of 1st Australian Conference on Broadband Wireless and Ultra Wideband*, pages 25–30, March 2006.
- [13] E. Sithirasenan, V. Muthukumarasamy, and D. Powell. IEEE 802.11i WLAN Security Protocol - A Software Engineer's Model. In *AusCERT '05: Proceedings of the 4th Asia Pacific Information Technology Security Conference*, pages 39–50, May 2005.
- [14] G. Vigna and R. A. Kemmerer. Netstat: A network-based intrusion detection system. *Journal of Computer Security*, 7(1), 1999.