An Early Warning System for 802.11i Wireless Networks

Elankayer Sithirasenan[1] and Vallipuram Muthukkumarasamy[2]
[1]Institute for Integrated and Intelligent Systems
[2]School of Infomation and Communication Technology
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 becoming more concerned about network security. The latest WLAN security protocol, the IEEE 802.11i assures rigid security for wireless networks with the support of IEEE 802.1X protocol for authentication, authorization and key distribution. However, users will remain skeptical unless they are confident and possess some form of assurance that the security mechanism is actually effective. In this view our Early Warning System (EWS) effectively confirms the legitimacy of the 802.11i security mechanism building confidence among the users. In this paper we outline our proposed WiFi-EWS for 802.11i wireless networks. Our system can effectively be used for anomaly detection and intrusion prevention. It has several levels of defense to protect the wireless networks from a range of possible threats. False alarms are raised only when all validations prove negative thus significantly reducing the number of false positives.

1. Introduction

Intrusion Detection Systems (IDS) are one of the fastest growing technologies within the network security space. Unfortunately, many organizations find it difficult to put these in effective use mainly because of the complexity of deployment, lack of information about its effective use and the amount of false positives. Our WiFi-EWS helps network security administrators, integrators and end-users to utilize their wireless networks to its limits and/or to meet the expectations of their organisation.

Rule-based IDS solutions aiming at detecting already known attacks by analysing traffic flow and looking for known signatures are very common [5, 7]. This requires such IDS to be under constant construction updating and modifying attack signatures and requiring considerable resources.

On the other hand it is possible to use anomaly based IDS solutions detecting not just known attacks but also unknown attacks and informing system administrators about possible network problems and helping them to troubleshoot [6, 1, 8].

Both these approaches have their own relative advantages and disadvantages. The rule-based approach has a low false-alarm rate, but it requires us to know the patterns of security attacks in advance and previously unknown attacks would go undetected. The anomaly-based approach can detect new attacks, but has a high false-alarm rate. However, all these methods are specific to wired networks and do not very well blend with wireless environments. In this respect our WiFi-EWS is developed specifically for 802.11i networks adopting a two-phase approach. Our WiFi-EWS combines anomaly-based methods together with data association techniques for preventing intrusions or to detect them before penetration. The main features of our approach are as follows:

- As a first level of defence our method looks for timing anomalies. A systematic learning mechanism is used to keep track of various timings for wireless transmissions.

- State transition analysis is used as the second level of defence. State tables are maintained for all participating hosts and are tracked for anomalies.

- Accumulating historical data and effectively querying them on-the-fly forms the third level of defence in our system. Very fast detection of outliers in large databases enables our system to quickly identify intruders.

To the best of our knowledge, this is the first work on an intrusion prevention system for IEEE 802.11i [4] based wireless networks. Use of multiple levels of defence makes our system robust and dependable. We have adopted fast data association techniques to identify outliers in our large wireless network traces, which makes our WiFi-EWS novel and unique with lessor number of false positives.

This paper is organized as follows. In Section 2 we give a brief overview of related work on network IDS. IEEE 802.11i security architecture is briefly explained in Section 3. Section 4 introduces the concept of our WiFi-EWS, some basic observations and properties. Section 5 concludes the paper.

2. Related Work

Unlike rule based analysis tools that pattern match sequences of audit records to the expected audit trials of known penetrations, the state transition analysis proposed by Ilgun et al. [5] focuses in an audit record independent rule-base that is easier to read than current 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 and Kemmerer [12] extended the above work and developed a tool for Network-based Intrusion Detection - NetSTAT aimed at real-time network 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. Although this system is effective in detecting attacks in wired networks it is not suitable for wireless network environments.

Hall et al. [3] introduce anaomaly based intrusion detection using mobility profiles. They discuss enhansing 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 stoten cell phones, given that the mobility behaviour 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 domain as the user to carry out an attack. Therefore the use of mobility profiles will not be suitable for wireless networks.

Paxson's [10] 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 a site's security policy. The events are compared with the security policy for anomalies.

Similar to the above work, our WiFi-EWS also focuses on tracking events for state transition analysis. Further, we also validate the wireless hosts for timing anomalies. However, our system does not merely raise alarms based on these outcomes. They perform an outlier-based data association analysis on historical data to find the support level of anaomalies before rasing alarms.

3. The IEEE 802.11i

Let us first take a brief look at the IEEE 802.11i standard. The standard defines two classes of security framework for IEEE 802.11 WLANs: RSN (Robust Security Network) and pre-RSN. A station is called RSN-capable equipment if it is capable of creating RSN associations (RSNA). Otherwise, it is pre-RSN equipment. The network that only allows RSNA with RSN-capable equipments is called a RSN security framework. The major difference between RSNA and pre-RSNA is the 4-way handshake. If the 4-way handshake is not included in the authentication / association procedures, stations are said to use pre-RSNA.

Fig. 1 shows an example RSNA establishment between a supplicant (STA) and the authenticator (AP) in an Extended Service Set (ESS). It assumes no use of pre-shared key. Flows 1-6 are the IEEE 802.11 association and authentication process prior to attaching to the authenticator. During this process, security information and capabilities could be negotiated using the RSN Information Element (IE). The Authentication in Flows 3 and 4 refer to the IEEE 802.11 open system authentication. After the IEEE 802.11 association is completed, the IEEE 802.1X authentication indicated in Flow 7 is initiated. If the supplicant and the authentication server authenticate each other successfully, both of them independently generate a Pairwise Master Key (PMK). The authentication server then transmits the PMK to the authenticator through a secure channel (for example, IPsec or TLS).

The 4-way handshake then uses the PMK to derive and verify a Pairwise Transient Key (PTK), guaranteeing fresh session key between the supplicant and the authenticator. This is indicated in Flow 8. Thereafter, the group key handshake is initiated as indicated by Flow 9. The group key handshake is used to generate and refresh the group key, which is shared between a group of stations and APs. Using this key, broadcast and multicast messages are securely exchanged in the

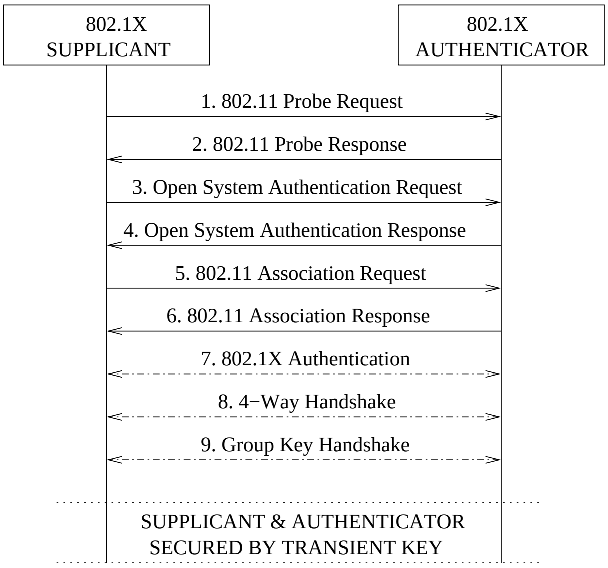

Figure 1. RSN Association

air.

The anomaly detection modules in the WiFi-EWS track all nine flows shown in Fig. 1 and make a decision on anomaly. We also use the software model [11] of the IEEE 802.11i security specification as the base model for detecting behavioral anomalies. The next section describes our proposed WiFi-EWS in detail.

4. The Proposed WiFi EWS

Fig. 2 illustrates the block diagram of the 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 the main component in our system with the ability of processing data association requests efficiently, preventing intrusions in real time. As mentioned earlier our WiFi-EWS has several levels of defence, 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 one or both anomalies a third level of defense is set off to validate 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. In the following sections we take a close look at the various modules of WiFi-EWS.

The packet capture module captures wireless data in promiscuous mode and delivers the captured management frames to the event engine. The event engine performs several reliability checks to assure that the management frames are regular. If the check fails the WiFi-EWS generates a log indicating the problem and discards the packet. On the other hand the event engine looks up the connection state associated with the management frame and generates the corresponding event and adds it to the master table for scrutiny by the subsequent modules. The following lines provide a sample list of the management frames captured from our experimental IEEE 802.11i wireless network.

```
1 0.00000000: STA1 - AP1 IEEE802.11 Authentication
2 0.00082400: AP1 - STA1 IEEE 802.11 Authentication
3 0.00253200: STA1 - AP1 IEEE 802.11 Association Request
4 0.00346300: AP1 - STA1 IEEE 802.11 Association Response
5 0.00527400: AP1 - STA1 EAP Request, Identity
6 0.20591200: STA1 - AP1 IEEE 802.11 Null function (No data)
7 0.22428900: STA1 - AP1 EAPOL Start
8 0.22706000: AP1 - STA1 EAP Request, Identity
9 0.33116600: STA1 - AP1 EAP Response, Identity
10 0.33717100: AP1 - STA1 EAP Request, EAP-TLS
11 0.41122400: STA1 - AP1 EAP Response, Identity
12 0.61183300: STA1 - AP1 TLS Client Hello
15 0.69990100: AP1 - STA1 EAP Request, EAP-TLS
16 0.70474100: STA1 - AP1 EAP Response, EAP-TLS
17 0.71026000: AP1 - STA1 TLS Server Hello, Certificate,
   Certificate Request, Server Hello Done
18 0.73782500: STA1 - AP1 TLS Certificate,
   Client Key Exchange, Certificate Verify, Change Cipher Spec,
   Encrypted Handshake Message
19 0.81907500: AP1 - STA1 TLS Change Cipher Spec,
   Encrypted Handshake Message
20 0.82157300: STA1 - AP1 EAP Response, EAP-TLS
21 0.83268000: AP1 - STA1 EAP Success
22 0.83557000: AP1 - STA1 EAPOL Key
23 0.86113200: STA1 - AP1 EAPOL Key
24 0.86614000: AP1 - STA1 EAPOL Key
25 0.87305300: STA1 - AP1 EAPOL Key
26 0.87734400: AP1 - STA1 IEEE 802.11 Data
27 0.87836000: STA1 - AP1 IEEE 802.11 Data
.
```

In the above traces STA1 represent the MAC address 0c:f1:3b:db:23 of a station and AP1 represent the MAC address 00:11:95:eb:60:51 of an access point. These traces could be appropriately related to the message flows shown in Fig. 1. The event engine deduces these traces, match them with the different events and forwards them to the anomaly detection modules for further processing. Table 1 shows the various events used in our system such as 11Auth, 11Assn, 1xStart etc. The 11Assn event is deduced from the Association-Request and Association-Response messages associated with a station. Similarly the 1xStart event corresponds to the EAP-Start message and the EAP-Request-Identity message.

As described in section 3, once PTK and GTK are installed on both the STA and AP they become associated, meaning they are synchronized. This post-association state is where the actual data transfer takes place and our study does not consider the wireless data

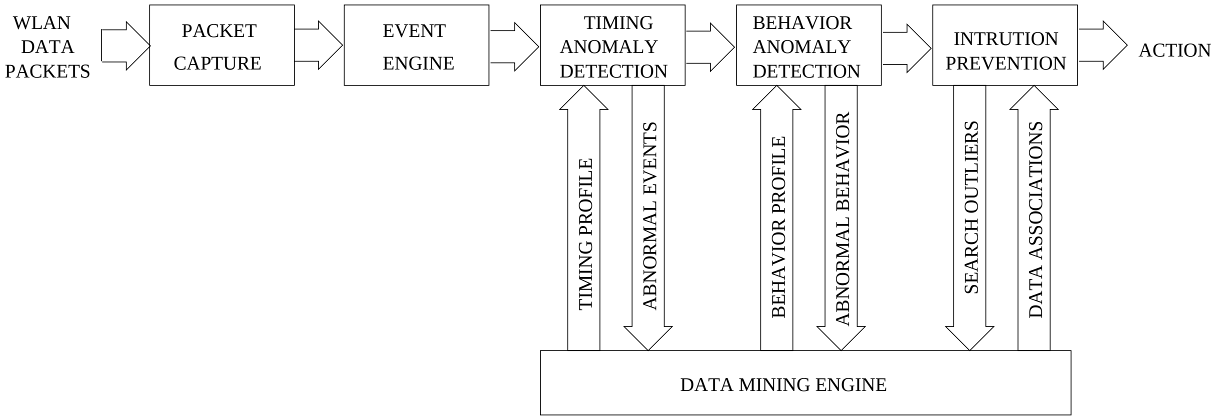

Figure 2. WiFi EWS Block Diagram

Message	Flow	Event
Authentication Request	$STA- > AP$	11Auth
Authentication Response	$AP- > STA$	
Association Request	$STA- > AP$	11Assn
Association Response	$AP- > STA$	
EAP Start	$STA- > AP$	1xStart
EAP Request Identity	$AP- > STA$	
TLS Client Hello	$STA- > AP$	Challenge
TLS Server Hello	$AP- > STA$	
TLS Cerrtificate	$STA- > AP$	1xComplete
EAP success	$AP- > STA$	
EAPOL Key	$AP- > STA$	ptkDerive
EAPOL Key	$STA- > AP$	
EAPOL Key	$AP- > STA$	ptkInstall
EAPOL Key	$STA- > AP$	

Table 1. Events Mapping

			Avg	Max	Min
Station	Access	Event	(ms)	(ms)	(ms)
STA1	AP1	11Auth	0.72	2.32	0.12
STA1	AP1	11Assn	0.91	3.20	0.25
STA1	AP1	1xStart	4.35	8.41	2.88
STA1	AP1	Challenge	91.22	101.24	62.35
STA1	AP1	1xComplete	95.52	123.11	70.27
STA1	AP1	PtkDerive	25.84	42.72	13.79
STA1	AP1	PtkInstall	12.70	33.62	6.64
STA1	AP2	11Auth	0.61	1.70	0.31
STA1	AP2	11Assn	1.21	5.20	0.32
STA1	AP2	1xStart	5.60	7.83	21.54
STA1	AP2	Challenge	83.34	129.5	60.45
STA1	AP2	1xComplete	91.84	110.68	87.81
STA1	AP2	PtkDerive	22.76	32.1	18.56
STA1	AP2	PtkInstall	17.54	21.98	11.32

Table 2. Timing Profile

during this period. Therefore message flows 26 and after in the above list does not fall within our analysis. However, all management frames transmitted during the post-association period needs to be tracked to establish systematic state transition. The WiFi-EWS is primarily concerned about the pre-association states between the STA and AP and traces every management frame transferred during this period. The post-association management frames of the roaming hosts are analysed to establish the transition from Associated state to Authenticating state.

The event engine also keeps track of missing and/or dubious message flows. Each event shown in Table 1 is associated with minimum of two message flows. However, due to intended or unintended reasons there can be situations where round trip messages may not reach the hosts. This type of situations could be the beginning of an intended attack on the wireless network and has to be tracked effectively. The event engine tracks such dubious message flows for analysis by the Intrusion Prevention module.

The first line of defense in WiFi-EWS is the examination of timing anomalies. The WiFi-EWS maintains a timing profile for every participating host in the wireless environment as shown in Table 2. Maximum, Minimum and Average timings are stored 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 associated response. In Table 2 we have shown a sample timing profile for the stations participating in our experimental network. This table is dynamically updated with new values of Average, Maximum and Minimum times depending on the current operational nature of the wireless environment.

The second level of defense in WiFi-EWS is the state transition analysis. In order to ascertain the state space of the participating hosts we used the RSN projection model developed in [11]. The first stage in state transition analysis is to compare events with that of the normal behavior of the hosts. A normally behaving host traverses all the legitimate states in the RSN projection model. If anomalies occur there can be situations where hosts fall into illegitimate states and do

Station	State	Access	State
STA1	Connecting	AP1	Connecting
STA1	Authenticating	AP1	Authenticating
STA1	Authenticated	AP1	Authenticated
STA1	Keying	AP1	Keying
STA1	Associated	AP1	Associated
STA2	Authenticating	AP1	Authenticating
STA2	Authenticated	AP1	Authenticated
STA2	Keying	AP1	Keying
STA2	Disconnected	AP1	Keying
STA3	Roaming	AP2	Roaming
STA3	Authenticating	AP2	Authenticating
STA3	Keying	AP2	Keying
STA3	Associated	AP2	Associated
STA4	Authenticating	AP2	Authenticating

Table 3. Behavioral Anomalies

{AP1, Authenticating, STA1, Disconnected, 98.4}
{AP1, Associated, STA3, Disconnected, 45.1}
{AP1, Authenticated, STA5, Connecting, 67.7}
{AP1, Disconnected, STA8, Authenticating, 45.6}
{AP1, Authenticated, STA12, Connecting, 67.7}
{AP1, Authenticating, STA17, Disconnected, 65.7}
{AP1, Associated, STA23, Disconnected, 67.2}
{AP1, Authenticated, STA25, Connecting, 75.5}
{AP1, Disconnected, STA36, Authenticating, 78.7}
{AP1, Authenticated, STA53, Connecting, 74.0}
{AP2, Disconnected, STA5, Authenticating, 79.7}
{AP2, Connecting, STA11, Disconnected, 92.4}
{AP2, Connecting, STA15, Authenticated, 94.0}
{AP2, Authenticated, STA17, Associated, 4.3}
{AP2, Associated, STA34, Connecting, 78.3}
{AP2, Connecting, STA45, Authenticated, 78.6}
{AP2, Authenticated, STA57, Associated, 7.8}
{AP2, Associated, STA64, Connecting, 68.8}

Table 4. Behavioral Associations

{1, AP2, STA5, STA6, STA12, STA15, STA17, STA19, ..STA25, STA34, STA35, 97.8}
{2, AP2, STA5, STA6, STA11, STA12, STA15, STA17, ..STA19, STA25, STA34, STA35, 98.2}
{3, AP2, STA4, STA5, STA6, STA11, STA12, STA15, ..STA17, STA19, STA25, STA34, 96.8}
{4, AP2, STA4, STA6, STA11, STA12, STA15, STA17, ..STA19, STA25, STA34, 97.2}
{1, AP2, STA1, STA6, STA11, STA12, STA15, STA17, ..STA19, STA25, STA34, 1.1}
{1, AP3, STA2, STA7, STA10, STA17, STA25, STA35, ..97.5}
{2, AP3, STA2, STA5, STA7, STA10, STA17, STA23, ..STA25, STA35, 98.2}
{3, AP3, STA2, STA7, STA10, STA17, STA23, STA25, ..STA35, 96.7}
{4, AP3, STA2, STA7, STA10, STA17, STA23, STA25, ..STA35, 96.4}

Table 5. Access Associations

not match our projection model. For example station STA1 in Table 3 behaves normal where it traverses all valid states and finally reaches the associated state. However, station STA2 does not exhibit normal behavior because from our projection model a station could not transit to disconnected state from the keying state. Nevertheless, this may have happened due to reasons beyond the control of the users. Therefore, WiFi-EWS does not instantly consider such anomalies as illegitimate, but they track such association and forward it to the Intrusion prevention module for further processing.

The third level of defense is the most important in WiFi-EWS and the module that executes this defense is called the intrusion prevention module. This module formulates critical decisions to verify the significance of the anomalies discovered in the previous modules. Hence this module plays an important role in maintaining our system reliable and efficient. In order to achieve our main goal of real time intrusion prevention, we have adopted an efficient querying technique proposed by Dehne et. al [2] to search our database for data associations. Details of how we maintain our databases and process it are reported elseware.

The intrusion prevention module executes a number of data association analyses to decide whether anomalies detected by the anomaly modules are significant or not. Firstly, the intrusion prevention module explores the connection states associated between both access point and station as shown in Table 4. Here, all states associated with stations and access points are investigated. The numerical values in each row indicate the remoteness [9] of the association. For example, if a station is found to exhibit both timing and behavioural irregularity we search the database for state space associations relating to the connection state of the station and the corresponding access point. Thus, if we find an association with significant outlying threshold we consider this an anomaly and issue a warning. On the other hand if an anomaly does not meet the required threshold we ignore it and update the database to add such states incrementing the overall count. However, if a situation arises where the database does not contain any state corresponding to that was searched we leave it for the discretion of the network administrator to add such states for future analysis.

Another form of data associations considered by our EWS is between access points and stations as shown in Table 5. This exploration gives us an indication of which stations are mostly associated with an access point. A station exhibiting behavioral anomaly is most likely to roam between several access points and hence associations between stations and access points are used to track stations which roam abnormally. This data association is also used to verify the anomalies and update the profiles appropriately.

The success of our WiFi-EWS will very much depend on the capabilities of the data mining engine. Although anomalies will give an initial warning towards a security breach, the legitimacy of such threats has to be instantly verified. Most anomaly based intrusion prevention methods produce a large number of false positive because of the deficiency in verifying the legitimacy of the security threats. In this context our main aim of introducing parallel computing techniques for effective data mining is to guarantee the legitimacy of every anomaly raised in real time.

In WiFi-EWS, an alarm could be raised by an anomaly detection module due to either an abnormal timing or an abnormal behaviour of the wireless host. However, this abnormality could be legitimate due to reasons beyond the control of the anomaly detection process. Therefore, we need another level of defence to verify the legitimacy of such abnormalities. In our WiFi-EWS the third level of defence, the intrusion prevention module does exactly this task of verifying the legitimacy of every detectable illegitimate functions of the wireless hosts reducing the number of false positives considerably.

5. Conclusion

In this paper, we have proposed a novel intrusion prevention mechanism for WiFi networks. The proposed WiFi-EWS is based on combining anomaly based methods with outlier based data association techniques. The initial experimental results obtained with the 802.11i based network are promising and confirming the concept of the proposed WiFi-EWS.

In the future work, the 3rd level of defense the intrusion prevention module will be fully implemented and the performance of the whole system will be tested.

References

[1] H. Debar, M. Becker, and D. Siboni. A neural network component for an intrusion detection system. *IEEE Computer Society Symposium on Research on Security and Privacy*, pages 240–250, May 1992.

[2] F. Dehne, T. Eavis, and A. Chaplin. Parallel Multi-Dimentional ROLAP Indexing. *3rd IEEE/ACM International Symposium on Cluster Computing and the Grid*, pages 86–93, May 2003.

[3] J. Hall, M. Barbeau, and E. Kranakis. Anomaly-based intrusion detection using mobility profiles of public transportation users. *IEEE International Conference on Wireless And Mobile Computing, Networking And Communications*, 2:17–24, August 2005.

[4] IEEE Std. 802.11i-2004 Part 11. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Medium Access Control (MAC) Security Enhancements.* IEEE, USA, 2004.

[5] 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.

[6] C. Ko, M. Ruschitzka, and K. Levitt. *Next-generation intrusion detection expert system. Technical Report SRI-CSL-95-07.* Computer Science Laboratory, SRI International, Menlo Park, CA, 1995.

[7] C. Ko, M. Ruschitzka, and K. Levitt. Execution monitoring of security-critical programs in distributed systems: A specification-based approach. *IEEE Symposium on Security and Privacy*, pages 175–187, May 1997.

[8] W. Lee. A data mining framework for building intrusion detection models. *IEEE Symposium on Security and Privacy*, pages 120–132, May 1999.

[9] S. Lin and D. E. Brown. *Outlier-Based Data Association: Combing OLAP and Data Mining, Technical Report.* Dept. of Systems Engineering, University of Virginia, 2002.

[10] V. Paxson. Bro: A system for detecting network intruders in real time. *7th USENIX Security Symposium*, pages 2–22, January 1998.

[11] E. Sithirasenan, V. Muthukkumarasamy, and D. Powell. IEEE 802.11i WLAN Security Protocol - A Software Engineer's Model. *4th AusCERT Asia Pacific Information Technology Security Conference*, pages 39–50, May 2005.

[12] G. Vigna and R. A. Kemmerer. NetSTAT: A Networkbased Intrusion Detection Approach. *14th Annual Computer Security Conference*, pages 25–34, December 1998.