Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

An Architectural Metrics Scorecard Based Approach to Intrusion Detection System Evaluation for Wireless Network

Mr. Rupinder Singh[1] and Dr. Jatinder Singh[2]

[1] Khalsa College, Amritsar, Punjab, India.

Received: 15 December 2011 Accepted: 3 January 2012 Published: 15 January 2012

Abstract

Wireless IDS architectural metrics are used to compare the intended scope, architecture of wireless IDS, and how they match the deployment architecture. These metrics can be used to evaluate the architectural efficiency of a wireless IDS and can help in designing efficient wireless IDS.Wireless IDS analyze wireless specific traffic including scanning for external users trying to connect to the network through access points and play important role in security to wireless network. Design of wireless IDS is a difficult task as wireless technology is advancing every day, Architectural metrics can play an important role in the design of wireless IDS by measuring the areas concern with the architecture of a wireless IDS. In this paper we describe a set of architectural metrics that are relevant to wireless IDS. A "scorecard" containing the set of values is used as the centerpiece of testing and evaluating a wireless IDS. Evaluation of a wireless IDS can be done by assigning score to various architectural metrics concern with wireless IDS. We apply our architectural metrics scorecard based evaluation approach to three popular wireless IDS Snort-wireless, AirDefense Guard, and Kismet. Finally we discuss the results and the opportunities for further work in this area.

Index terms— Architectural Metrics, Wireless, Metrics, IDS, and Scorecard.

1 Introduction

new and exciting world has been opened by wireless. Its technology is advancing every day and its popularity is increasing. The biggest concern with wireless, however, has been its security, for some time wireless has had very poor, if any, security on a wide-open medium. Along with improved encryption schemes, a new solution to help combat this problem is the Wireless Intrusion Detection System (WIDS). An Intrusion Detection System (IDS) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station **??**Wikipedia, 2012). A wireless IDS performs this exclusively for the wireless network. This system monitors traffic on network looking for threats and alerting personnel to respond.

Lord Kelvin said "If you cannot measure it, you cannot improve it". This fact also applies to wireless network security issues. An activity cannot be managed if it cannot be measured, this is a widely accepted management principle and security falls under this rubric. Metrics can be an effective tool for security providers to discern the effectiveness of various components of their security programs. Metrics can play an important role in the designing of wireless IDS. Security Metrics that are related to wireless network are hard to generate because the discipline itself is still in the early stages of development. There is not yet a common vocabulary and not many documented best practices to follow [1].

This paper provides an architectural metrics scorecard based approach to evaluate Intrusion Detection Systems that are currently popular for wireless in the commercial sector. We describe a testing methodology we developed to evaluate wireless IDS by assigning score to various architectural metrics concern with it. The approach followed

in this paper do not compare wireless IDS against each other, but against a set of architectural metrics concern with wireless IDS.

The generalized approach of this paper will allow systems with any wireless requirements to tailor evaluation of ID technologies to their specific needs. Since evaluation is against a static set of architectural metrics the evaluation may be extended for other metrics like logistical metrics, performance metrics, quality metrics etc. The standard approach of comparison used in this paper also gives us scientific repeatability.

2 II. Snort, Airdefense Guard and Kismet Wireless Ids

In order to explain architectural metrics scorecard based evaluation approach to wireless IDS, we choose three wireless IDS namely Snort-wireless, AirDefense Guard, and Kismet as these are one of the most popular and works on different technology.

3 a) Snort Wireless IDS

Snort is an open source network intrusion detection and prevention system (IDS/IPS) that combines the benefits of signature, protocol, and anomaly-based inspection, and is the most widely1 2012 (D D D D)

deployed IDS/IPS technology worldwide. With millions of downloads Snort has become the de facto standard for IDS/IPS [4]. Snort-wireless allows for custom rules to be created based on framing information from a wireless packet. It also contains rules to attempt to find rogue access points, war drivers, and ad hoc networks.

Snort-wireless works by implementing a detection engine that allows registering, warning, and responding to attacks previously defined. Snort-wireless is available under GPL (General Public License) and runs under Windows and GNU/Linux. It is among the most widely used, has a number of predefined signatures and continuously updated. Snort wireless can be configured in three modes namely sniffer, packet logger, and network intrusion detection. In addition to all of these basic Snort-wireless features, Snort-wireless can be set up to send real-time alerts. This provides with the ability to receive alerts in real time, rather than having to continuously monitor Snort system. Snort is like a vacuum that takes packets and allows to do different things.

4 b) AirDefense Guard Wireless IDS

AirDefense Guard is a wireless IDS that provides advanced intrusion detection for wireless LANs based on signature analysis, policy deviation, protocol assessment policy deviation and statistically anomalous behavior. AirDefense Guard is able to respond to attacks with Active Defense technology, which interfaces with the access points to disconnect the attackers connection to the WLAN.

AirDefense can be used to identity theft. This is done by stealing an authorized MAC address, an intruder has full access to the network. However, AirDefense tracks the digital fingerprints vendor-specific characteristics and personal trademarks of authorized users to identify intruders in the network. AirDefense can be used to detect Denial-of-Service (DoS) attacks. AirDefense is able to quickly recognize the early signs and protocol abuses of a DoS attack that jams the airwaves and shuts down a wireless LAN. AirDefense can also be used to detect Man-in-the-Middle attacks. Posing as an access point, intruders can force workstations to disassociate from authorized access points and route all traffic through the intruder. The intruder can then gain access to the network by posing as an authorized user and simultaneously operating on multiple channels. AirDefense detects man-in-themiddle attacks and ensure that access points only operate on set channels and proper protocols are used. c) Kismet Wireless IDS Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will works with any wireless card that supports raw monitoring mode, and can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet also supports plugins that allows sniffing other media such as DECT.

Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting hidden networks, and inferring the presence of nonbeaconing networks via data traffic **??**8]. Kismet wireless IDS without sending any loggable packets is able to detect the presence of both wireless access points and wireless clients, and associate them with each other. Unlike most other wireless network detectors. Kismet has the ability to log all sniffed packets and save them in a tcpdump /Wireshark or Airsnortcompatible fileformat. Kismet also captures PPI headers. Kismet also has the ability to detect default or "not configured" networks, probe requests, and determine what levels of wireless encryptions is used on a given access point. Kismet also supports logging of the geographical coordinates of the network if the input from a GPS receiver is additionally available **??**12].

5 III.

6 Architectural Metrics Scorecard

Based Approach a) Developing Scorecard

Centerpiece of testing and evaluating wireless IDS will be a "scorecard" containing the set of architectural metrics and their definitions. Each metric can have low (+), average (++), or high (+++) score, where higher scores will be interpreted as more favorable ratings.

The architectural metrics used are general characteristics that are relevant to architecture of a wireless IDS. The method used for observing each architectural metric value can be either analysis (source code analysis) or open source material (such as specifications, white papers or reviews provided by vendors or users). We use open

source material to analyze each architectural metrics for wireless IDS. We examine publicly available research papers, reports, product documentation, published conference material (proceedings) and other material available for public review. b) Architectural Metrics for a Wireless IDS Architectural metrics are used to compare the intended scope and architecture of wireless IDS and how they match the deployment architecture. These metrics evaluate the architectural efficiency of a Wireless IDS [13]. The metrics defined in this area are shown in The difficulty of altering the sensitivity of a wireless IDS in order to achieve a balance between false positive and false negative error rates at various times and for different environments.

7 Required Data Storage Capacity

The amount of disk space needed to store logs and other application data.

8 Load Balancing Scalability

It measures the ability of a wireless IDS to partition traffic into independent, balanced sensor loads.

9 Multiple Sensor Support

The cardinality of sensors supported.

10 Reordering and Stream Reassembly

It can be used to find an attack that has been artificially fragmented and transmitted out of order.

11 State Tracking

This metric is useful in hardening wireless IDS against storms of random traffic used to confuse it.

12 Data Pool Selectability

This metric is used to define the data source to be analyzed for intrusions.

13 System Throughput

Maximal data input rate that can be processed successfully by the wireless IDS. In this section we will apply above mentioned approach to popular wireless IDS Snort-wireless, AirDefense Guard, and Kismet. We choose these three for evaluation as they are one of the most widely used and have different ways of working. Below with table 2 we describe how scores to architectural metrics related to these three wireless IDS are assigned.

14 Architectural Metrics

15 Snort wireless

AirDefense

Architectural metric Adjustable Sensitivity can be assigned score depending on the following criteria: Low Score (+): No Adjustability. Average Score (++): Adjustability via static methods. High Score (+++): Intelligent, dynamic Adjustability.

Snort-wireless makes use of the SSL Dynamic Preprocessor (SSLPP), which decodes SSL and TLS traffic and optionally determines if and when Snortwireless should stop inspection of it. Encrypted traffic is ignored by Snort-wireless for both performance reasons and to reduce false positive and false negative error rate **??**15]. So, Snort-wireless gets a high score (+++) for metric adjustable sensitivity. Kismet wireless provides alerts based on fingerprints (specific nets tumbler versions). In an attempt to disclose the SSID of a network, Nets tumbler sends out unique packets. This is not done in all situations, but when it is detected the potential for false positives is very low **??**16]. So, kismet gets average score for metric adjustable sensitivity. As described in [17] Air defense guard delivered a false positive for a Nets tumbler scan that turned out to be one of test laptops pinging an AP. Air Defense acknowledged that its Nets tumbler, signature needs some tweaking. So, it gets average score for metric adjustable sensitivity.

Architectural metric Required Data Storage Capacity can be assigned score depending on the following criteria:

Low Score (+): Large capacity storage needed to store log and other files.

Average Score (++): Medium capacity storage needed to store log and other files.

High Score (+++): Low capacity storage needed to store log and other files. Databases are used with Snort wireless to store log and alert data. Logging data to files in the disk is fine for smaller applications. However, keeping log data in disk files is not appropriate when there are multiple Snort-wireless sensors or there is need to keep historical data as well. Databases also allow to analyze data generated by Snort-wireless sensors. Snort-wireless uses rules stored in text files that can be modified by a text editor. Rules are grouped in categories. Rules belonging to each category are stored in separate files. These files are then included in a main configuration file called snort.conf. Alerts are also stored in log files or databases where they can be viewed later on by security experts. Snort wireless needs a large database as its rules grows and gets a for this metric. Airdefense guard

makes use of average data storage. Kismet wireless makes use of predefine rules and therefore needs less storage to store files.

Architectural metric Load Balancing Scalability can be assigned score depending on the following criteria: Low Score (+): No load balancing scalability. Average Score (++): Low load balancing scalability. database is not strictly "real-time". There is a certain delay which depends upon frequency of uploading data using SCP to the centralized database server. This arrangement is shown in Figure **??** [7].

Figure **??** : Distributed Snort-wireless installation with the help of tools like SCP and Barnyard [7] Collaborative Intelligence Architecture (DCIA), pioneered by Air Defense, to provide the most comprehensive wireless intrusion protection. DCIA uses a dedicated network of sensors and embedded client based agents that continuously monitor the airwaves and wireless activity for attacks and policy violations. In addition, the sensors use an intelligent channel scanning algorithm to detect traffic across the RF spectrum. So, Air Defense guard also gets a +++ score. Like Snort-wireless and Air defense Kismet wireless also have a support to multiple sensors.

Architectural metric Reordering and Stream Reassembly can be assigned score depending on the following criteria:

Low Score (+): No capability to find an attack that has been artificially fragmented and transmitted out of order.

Average Score (++): Very less capability to find an attack that has been artificially fragmented and transmitted out of order.

High Score (+++): Highly capable to find an attack that has been artificially fragmented and transmitted out of order.

The open source IDS Snort wireless implement target-based analysis with the frag3 preprocessor. Frag3 is able to reassemble overlapping fragments using the same policy as the destination host. A user configures the IDS to apply specific fragmentation reassembly policies for individual hosts or networks. Then, when the Snort sees overlapping fragments bound for any of these hosts, it knows the appropriate reassembly policy to apply-allowing both Snort and the destination host to reassemble the fragments identically. If the bandwidth being passed by the network interface associated with a Snort-wireless instance is greater than it can handle, more instances of Snortwireless can be launched and the traffic can be load balanced across the instances. An Adaptive load balancing architecture for snort is discussed in [18]. So, snort wireless gets a +++ score for this metric.

Motorola AirDefene guard wireless IDS clients use a sophisticated load-balancing algorithm when too many clients attempt to connect to a particular access point. The clients use a beacon element to perform preemptive roaming and load balancing, thereby moving from a heavily loaded AP to one that is less loaded. Kismet wireless is not as capable as Snortwireless and AirDefense Gurad for load balancing scalability.

Architectural metric Multiple Sensor Support can be assigned score depending on the following criteria:

Low Score (+): Very less number of sensors supported.

Average Score (++): Average number of sensors supported.

High Score (+++): Large number of sensors supported.

A corporate environment probably have multiple locations and there is need to install Snort-wireless sensors. There are multiple ways to setup and install Snort-wireless in the enterprise as a distributed IDS. One method is to connect multiple sensors to the same centralized database. All data generated by these sensors is stored in the database. A user then uses a web browser to view this data and analyze it.

In an alternate mechanisms, Snort-wireless sensors do not have a direct connection to the database server. The sensors may be configured to log to local files. These files can then be uploaded to a centralized server on a periodic basis using utilities like SCP. The only problem with this approach is that the data in the Snort wireless gets a +++ score for this metric. The Air Defense solution is based on a Distributed Snort wireless gets a +++ score as it is able to find an attack that has been artificially fragmented and transmitted out of order. AirDefense Guard and Kismet wireless are also capable for out of order attaks.

Architectural metric State Tracking can be assigned score depending on the following criteria:

Low Score (+): No capability to detect storms of random traffic used to confuse wireless IDS.

Average Score (++): Less capability to detect storms of random traffic used to confuse wireless IDS.

High Score (+++): High capability to detect storms of random traffic used to confuse wireless IDS.

Snort wireless gets a high score for metric state tracking as Snort wireless provides many configuration and command line options to detect storms of random traffic that can be specified in the snort configuration file. Table 3 describes such commands. AirDefense guard and Kismet wireless are also able to track state and gets a +++ score.

Architectural metric Data Pool Selectability can be assigned score depending on the following criteria:

Low Score (+): Poor capability to detect the data source to be analyzed for intrusion.

Average Score (++): Average capability to detect the data source to be analyzed for intrusion.

High Score (+++): Highly capable to detect the data source to be analyzed for intrusion Snort wireless gets a +++ score for metric data pool selectablity as Snort is a very complex pattern matcher geared toward detecting patterns of network attack traffic. On any If Snort has to work with a high speed connection, then there is need to use unified logging and a unified log reader such as barnyard. This allows Snort-wireless to log alerts in a binary form as fast as possible while another program performs the slow actions, such as writing to a database.

AirDefense Guard and Kismet wireless process less data input rate as compare to snort wireless and both gets ++ score for the metric system throughput. Figure 2 shows score of Snort-wireless, Airdefense and Kismet IDS. IV.

16 Conclusion and Future Work

Unwanted activities on a wireless network can be detected by a wireless IDS. Architectural design of a wireless IDS is a difficult task as the technology of design of wireless network is changing at a pace which brings additional challenges in the design of wireless IDS. This paper provides an architectural metrics scorecard based approach that can be used for evaluating a wireless IDS in order to find out the areas in which wireless IDS is weak and needs improvement. Depending upon the requirements of the system these metrics me given priorities and appropriate wireless IDS may be selected after developing the scorecard.

In this paper we define various architectural metrics concern with wireless IDS and a scorecard method to evaluate a wireless IDS by assigning scores to various architectural metrics. We use our evaluation methodology to test popular wireless IDS Snort-wireless, Air Defense Guard, and Kismet. This paper defines commonly used architectural metrics that are important to a wireless IDS, but a lot is required to be done to find out more ones like anomaly based, autonomous learning, Host/OS security, interoperability, package contents, process security, signature based, visibility etc. More architectural metrics and their definitions can be defined as lessons are learned while evaluating a wireless network. Future work also includes applying the evaluation methodology to other metrics concern with wireless IDS like logistical metrics, performance metrics, quality metrics etc.

17 Enable_decode_drops

Enables the dropping of bad packets identified by decoder (only applicable in inline mode).

18 Enable_tcpopt_e xperimental_dro ps

Enables the dropping of bad packets with experimental TCP option. (only applicable in inline mode).

19 Enable_tcpopt_o bsolete_Drops

Enables the dropping of bad packets with obsolete TCP option. (only applicable in inline mode).

20 Enable_tcpopt_tt cp_drops

Enables the dropping of bad packets with T/TCP option. (only applicable in inline mode).

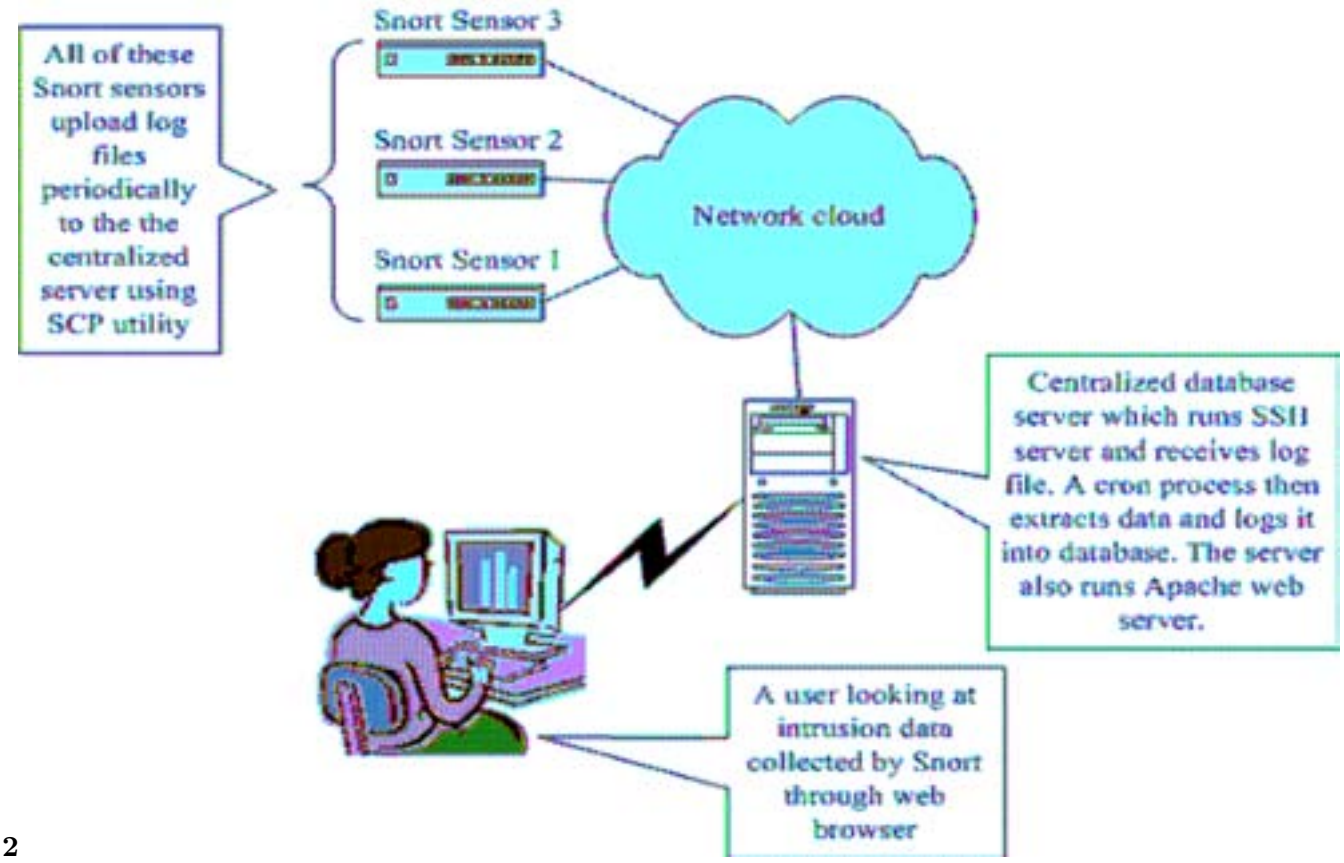
21 Enable_tcpopt_d rops

Enables the dropping of bad packets with bad/truncated TCP option (only applicable in inline mode).

22 Enable_ipopt_dr ops

Enables the dropping of bad packets with bad/truncated IP options (only applicable in inline mode). [1]

Figure 1:



2

Figure 2: Figure 2 :

1

. Other Architectural metrics that may be
included are: Anomaly Based, Autonomous Learning,
Host/OS Security, Interoperability, Package Contents,
Process Security, Signature Based, and Visibility [6].

[Note: E]

Figure 3: Table 1

1

Figure 4: Table 1 :

2

3
Volume XII Issue XI Version I
D D D D) E
(
Global Journal of Computer Science and Technology

[Note: © 2012 Global Journals Inc. (US)]

Figure 5: Table 2 :

3

Architectural metric System Throughput can be
assigned score depending on the following criteria:
Low Score (+): Wireless IDS can successfully
process less data input rate.
Average Score (++): Wireless IDS can
successfully process average data input rate.
High Score (+++): Wireless IDS can
successfully process high data input rate.

Figure 6: Table 3 :

[Freelance et al. (May 09)] , Harrykar Freelance , " Harrykar's Techies Blog , Snort , Ids , Nsm Ips . May 09. p. 31.

[Enterprise Wlan Design Guide (2008)] , Motorola Enterprise Wlan Design Guide . http://www.scantexas.com/asset/support/Motorola%20Enterprise%20WLN%20Design%20Guide.pdf November 2008.

[Fink et al. (2002)] 'A Metrics -Based Approach to Intrusion Detection System Evaluation for Distributed Real -Time Systems'. G A Fink , B L Chappell , T G Turner , K F O'donoghue . *WPDRTS* April 2002.

[Singh and Singh (2011)] 'A Metrics-Based Approach to Intrusion Detection System Evaluation for Wireless Network'. Rupinder Singh , Dr Jatinder Singh . *International Journal of Education and Applied Research (IJEAR)* 2249-4944. Jul.-Dec., 2011. 1 (1) .

[Alam et al.] *Adaptive load balancing architecture for snort*, M Alam , Qasim Javed , M Akbar . http://www.geocities.ws/raza_nust/incc.pdf

[Gómez et al. ()] 'Design of a Snor -Based Hybrid Intrusion Detection System'. J Gómez , C Gil , N Padilla1 , R Baños , C Jiménez . *Part II*, 2009. 2009. 5518.

[Rafeeq Ur Rehman ; Apache and Mysql] *Intrusion Detection System with Snort Advanced IDS Techniques Using Snort*, Rafeeq Ur Rehman ; Apache , Php Mysql , Acid . http://ptgmedia.pearsoncmg.com/images/013147333/downloads/0131407333.pdf Prentice Hall. p. .

[Savola (2010)] 'On the Feasibility of Utilizing Security Metrics in Software Intensive Systems'. Reijo Savola . *IJCSNS* January 2010. 10 (1) .

[Northcutt] *Snort 2.1 Intrusion Detection*, Stephen Northcutt . Shroff Publishers. ISBN p. . (Second Edition)

[SNORT Users Manual 2.9.0, Snort Project (2011)] *SNORT Users Manual 2.9.0, Snort Project*, March 2011.

[SNORT Users Manual 2.9.1, the Snort Project (2011)] *SNORT Users Manual 2.9.1, the Snort Project*, http://www.networkcomputing.com/wireless/22962263?printer_friendly=this-page September 20. 2011.

[Boob and Jadhav (2010)] 'Wireless Intrusion Detection System'. Snehal Boob , Priyanka Jadhav . *International Journal of Computer Applications* August 2010. 5 (8) p. .