USER REQUIREMENTS WEIGHT BASED APPROACH TO IDS SELECTION FOR WLAN

Rupinder Singh[†], Dr. Jatinder Singh[‡]
[†]Rupinder Singh, Khalsa College, Amritsar, Punjab, India.
rupi_singh76@yahoo.com
[‡]Dr. Jatinder Singh, DAV University, Jalandhar, Punjab, India.
bal_jatinder@rediffmail.com

Abstract - A variety of featured packed Wireless Intrusion Detection System (WIDS) products are available in the market. They include commercial as well as open source products. It is for user to decide which will be the best WIDS solution for their network. There is never one solution that works for everything so user has to compare the capabilities of each along with budget, knowledge and needs to find one that works best for them. This paper provides a user requirements weight based approach to IDS selection for WLAN. In this approach first all possible user WIDS requirements and WIDS metrics are listed, then for each WIDS requirement we find the concern metric(s). User lists their WIDS requirements in a partial ordering from least important to most. Requirements are usually stated in positive form or converted to the positive form. Next, the first requirement (i.e. least important) is assigned the lowest weight (e.g., one). Other requirements may be assigned increasing weights in proportion to their relative importance. Once the requirements are weighted, each WIDS metric is assigned a weight that is equal to the sum of the weights of the requirements it contributes to. WIDS metrics are arranged in descending order where metric with the highest weight is at the top. Appropriate WIDS tool may be selected after matching the metrics weight and WIDS features. In the end of the paper we discuss scope for the future work in this area.

Keywords: WIDS, IDS, WLAN, metrics, open source, partial ordering, and tool.

I. INTRODUCTION

Security problem are not purely technical, organization policy decisions decides about the user's requirements. The goals, acceptable uses, and constraints on the system are decided by organizational policy regarding security. It is organizational agreement that is going to decide what to monitor, when to alert and whom to alert, or up to what degree of threat a potential intrusion presents.

Networking of the computers has given rise to the issue of network security. The need of security program was increased with the evolution of the internet. Intrusion Detection Systems (IDS) has emerged as an important security product. An 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, 2016). Wireless has opened many new possibilities for expanding networks. It has amazing potential. Since wireless is a new technology it also has several vulnerabilities. Products like Wireless Intrusion Detection System (WIDS) have come about that address many of these. WIDS products are available from both commercial and the open-source, having their own advantages and disadvantages.

As variety of WIDS products are available in the market, so it becomes difficult to choose one of them as it's a complex and time consuming process. This becomes more difficult if the organization does not have a corporate security program. WIDS selection decision should not be made quickly, lightly, or without having a firm understanding of the technology, options, or the potential impacts. In this paper we provide a user requirements weight based approach to IDS selection for WLAN. In this approach first all possible user WIDS requirements and WIDS metrics are listed. Then for each WIDS requirement we find the concern metric(s). User lists their WIDS requirements in a partial ordering from least important to most. Requirements are usually stated in positive form or converted to the positive form. Next, the first requirement (i.e. least important) is assigned the lowest weight (e.g., one). Other requirements may be assigned increasing weights in proportion to their relative importance. Once the requirements are weighted, each WIDS metric is assigned a weight that is equal to the sum of the weights of the requirements it contributes to. WIDS metrics are arranged in descending order where metric with the highest weight is at the top. Appropriate WIDS tool may be selected after matching the metrics weight and WIDS features.

II. CHOOSING RIGHT WIDS

A variety of WIDS products are available in the market with different features and capabilities. They work on different platforms and many of them are freely available under GPL (General Public License). The decision process for selecting a WIDS can be divided into the following steps:

1. Identify the need for WIDS by performing risk assessment of the organization.
2. Understanding technical environment of organizations wireless network.
3. Perform cost benefit analysis.
4. Apply user requirements weight based approach to choose right WIDS product.
5. Perform strategic deployment of WIDS.
6. Monitoring and maintenance of WIDS.

Because of the limitations we will concentrate only on step 4 of the above mentioned process. The decision of selecting best WIDS solution for the network totally depends on its users. One solution is never going to work for everything, therefore user has to compare the capabilities of each WIDS product along with the budget and knowledge which in term will help them in finding the needs for the best solution. User requirements weight based approach involves following steps:

i) Collect user WIDS requirements.

ii) Assign lowest weight (e.g., one) to least important requirement.

iii) Other requirements may be assigned increasing weights in proportion to their relative importance. There is also possibility of duplicate weights.

iv) Arrange these requirements from least important to most one.

v) Once the requirements are weighted, each WIDS metric is assigned a weight that is equal to the sum of the weights of the requirements it contributes to.

vi) Arrange WIDS metrics in descending order.

vii) Select appropriate WIDS tool.

User requirements for WIDS product may be collected by asking following questions to the user:

1. What is the size of the organizations wireless network?
2. Whether there is need for complete hardware product, or complete software product, or a combined hardware and software product?
3. Whether the WIDS product needed is to be commercial system or open source system?
4. What should be the WIDS policy behind intrusion detection?
5. What should be the attack detection capability of WIDS product?
6. How much it should be difficult to install, configure, and adjust WIDS product?
7. What Platform and other resources could be provided for proper functioning of WIDS?
8. How much performance of WIDS is expected?
9. How much reliable should be WIDS product?
10. How much correct reporting and recovery is expected from WIDS product?
11. What should be the interaction of WIDS product with the firewall and router?
12. What should be WIDS setting as per user environment?
13. How license Management is expected?
14. What and when updates are expected?
15. How much disk space could be provided to store logs and other application data?
16. How much WIDS stress tolerance is expected?
17. What kind of wireless cards are used in the network?
18. What network IP range is provided?
19. What compatibility of WIDS with other products is expected?
20. What should be the level of administration for WIDS?
21. What should be the WIDS product lifetime?
22. What kind of technical support is expected?
23. How much clarity of reports is expected?
24. Is information going to be shared?

25. How previous session data is to be recorded?
26. Is there need to extend the network in the future?
27. What should be the maximal input data processing rate of WIDS product?

After noting the WIDS user requirements by asking above question, user may be asked to arrange these requirements in an order as per requirement so that appropriate weights may be assigned to the requirements. Depending on the requirements user may leave any of the above questions or may add to the list. Once the requirements are fixed, approach discussed in the paper may be applied for selecting appropriate WIDS product.

III. WIDS METRICS

In this section of the paper we will be discussing in greater detail the metrics that are most applicable to WIDS. The metrics set for WIDS will be divided into Logistical (class 1), Architectural (class 2), and Performance (class 3) one as shown in figure 1 and is described below in detail [1].

Logistical Metrics (Class 1): Logistical metrics are used to measure expense, maintainability, and manageability of a wireless IDS. The metrics we define applicable to wireless IDS in this area are shown in Table 1.

Table 1 includes only the selected logistical metrics. Other logistical metrics that can be included are: Documentation Quality, Available Copy Evaluation, Administration Level, Product Lifetime, Quality of Technical Support etc [19].

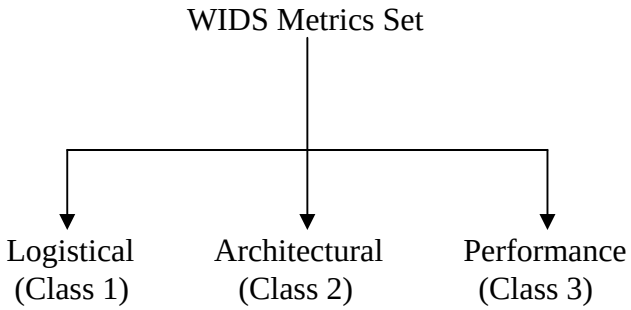

Figure 1: Classification of WIDS metrics [1].

Table 1: Selected Logistical Metrics

Logistical Metrics	Description
Distributed Management	Determining the distribution capabilities of a WIDS. It is used to determine up to what extent a Wireless IDS supports distributed management.
Configuration Difficulty	The difficulties a user faces while installing and configuring a WIDS.
Policy Management	The difficulty in setting security and intrusion detection policies for a WIDS.
License Management	The difficulty in obtaining, updating and extending licenses to a WIDS.
Availability of Updates	The availability of updates of behavior profiles and cost of product upgrades.
Platform Requirements	System resources needed to implement a WIDS.
Availability of Technical Support	It defines the quality of technical support provided by WIDS supplier.

Metrics like Configuration Difficulty, Policy Maintenance, License Management etc. are applicable because products having low features in these areas would not be easy to use in a distributed environment with multiple sensors. Platform Requirements give an indication of the system resources that will be consumed by the WIDS in the resource-critical wireless environment.

Architectural Metrics (Class 2): Architectural metrics are basically used to compare the intended scope and architecture of the WIDS and how they match the deployment architecture. These metrics evaluate the architectural efficiency of a WIDS. The metrics defined in this area are shown in Table 2 [20].

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

Table 2: Selected Architectural Metrics

Architectural Metrics	Description
Adjustable Sensitivity	The difficulty of altering the sensitivity of a WIDS in order to achieve a balance between false positive and false negative error rates at various times and for different environments.
Required Data Storage Capacity	The amount of disk space needed to store logs and other application data.
Load Balancing Scalability	It measures the ability of a WIDS to partition traffic into independent, balanced sensor loads.
Multiple Sensor Support	The cardinality of sensors supported.
Reordering and Stream Reassembly	It can be used to find an attack that has been artificially fragmented and transmitted out of order.
State Tracking	This metrics is useful in hardening WIDS against storms of random traffic used to confuse it.
Data Pool Selectability	This metrics is used to define the source data to be analyzed for intrusions.
System Throughput	It is used to define the maximal data input rate that can be processed successfully by the WIDS.
Interoperability	It defines the compatibility of WIDS with other similar products

Performance Metrics (Class 3): Performance metrics are used to measure the ability of a WIDS to perform a particular task and to fit within the performance constraints. These metrics measure and evaluate the parameters that impact the performance of the WIDS [1]. The metrics defined in this area are shown in Table 3 [21].

Table 3 includes only the selected Performance metrics. Other Performance metrics that can be included are: Analysis of Intruder Intent, Clarity of Reports, Effectiveness of Generated Filters, Evidence Collection, Information Sharing, User Alerts, Program Interaction, Threat Correlation, and Trend Analysis.

Table 3: Selected Performance Metrics

Performance Metrics	Description
False Positive Ratio	This is the ratio of alarms that are wrongly raised by the WIDS to the total number of transactions.
False Negative Ratio	This is the ratio of actual attacks that are not detected by the WIDS to the total number of transactions.
Cumulative False Alarm Rate	The weighted average of False Positive and False Negative ratios.
Induced Traffic Latency	It measures the delay in the arrival of packets at the target network in the presence and absence of a wireless IDS.
Stress Handling and Point of Breakdown	The point of breakdown is defined as the level of network or host traffic that results in a shutdown or malfunction of IDS.
IDS Throughput	This metrics defines the level of traffic up to which the WIDS performs without dropping any packet.
Depth of System's Detection Capability	It is defined as the number of attack signature patterns and/or behavior models known to it.
Breadth of System's Detection Capability	It is given by the number of attacks and intrusions recognized by the IDS that lie outside its knowledge domain.
Reliability of Attack Detection	It is defined as the ratio of false positives to total alarms raised.
Possibility of Attack	It is defined as the ratio of false negatives to true negatives.
Consistency	It is defined as the variations in the performance of a WIDS.
Error Reporting and Recovery	The ability of a WIDS to correctly report and recover.
Firewall Interaction	The ability of a WIDS to interact with the Firewall systems.

User Friendliness	The ability of a WIDS to configure according to user's environment.
Router Interaction	Degree of interaction of a WIDS with the router.
Compromise Analysis	It is the ability to report the extent of damage and compromise due to intrusions.
Induced Traffic Latency	It is the degree to which traffic is delayed by the WIDS presence or operation.
Session Recording and Playback	It is the ability of WIDS to record previous session and to play them

IV. MAPPING USER REQUIREMENTS TO METRIC(S)

The metrics related with each of possible user requirement are given in table 4. It indicates what metrics are contributing to fulfill a particular requirement. For example size of user wireless network is concern with the metrics Distributed Management, Configuration Difficulty, Platform Requirements, Adjustable Sensitivity, Load Balancing Scalability, and Multiple Sensor Support shown in the column corresponding to requirement number 1. The purpose is to help user in making a correct choice to WIDS product.

With figure 2, we provide notations that will be used to represent user requirements and WIDS metrics relationship. Figure 3 gives user requirement to WIDS metric weighting example. As in figure 3 metric configuration difficulty gets highest weight, so the WIDS product having least difficulty in configuring appears to be the best solution to the user environment in this example. It is also possible that some of the metrics discussed above may not contribute to any of the user requirement. As wireless technology is changing more metrics and questionnaires may be added to the above approach.

Table 4: User requirements and metrics relation.

Question number for gathering User requirement	**Concerned WIDS metric(s)**
1	Distributed Management, Configuration Difficulty, Platform Requirements, Adjustable Sensitivity, Load Balancing Scalability, Multiple Sensor Support
2	Configuration Difficulty, Policy Management, Platform Requirements
3	Configuration Difficulty, License Management
4	Policy Management
5	Reordering and Stream Reassembly, State Tracking, Data Pool Selectability.
6	Distributed Management, Configuration Difficulty, Adjustable Sensitivity, User Friendliness
7	Distributed Management, Platform Requirements, Required Data Storage Capacity
8	Distributed Management, Induced Traffic Latency, IDS Throughput, Depth of System's Detection Capability, Breadth of System's Detection Capability, Reliability of Attack Detection, Possibility of Attack, Consistency, Induced TrafficLatency
9	False Positive Ratio, False Negative Ratio, Cumulative False Alarm Rate
10	Required Data Storage Capacity, Error Reporting and Recovery
11	Configuration Difficulty, Firewall Interaction, Router Interaction
12	Configuration Difficulty, Policy Management, License Management, User Friendliness
13	License Management, Multiple Sensor Support
14	Availability of Updates
15	Distributed Management, Platform Requirements, Required Data Storage Capacity
16	Compromise Analysis, Stress Handling and Point of Breakdown
17	Platform Requirements
18	Distributed Management, Configuration Difficulty, Multiple Sensor Support
19	Interoperability
20	Distributed Management, Configuration Difficulty, Policy Management, Multiple Sensor Support
21	License Management

22	Availability of Technical Support
23	Error Reporting and Recovery
24	Distributed Management, Multiple Sensor Support
25	Session Recording and Playback
26	Load Balancing Scalability, Multiple Sensor Support
27	System Throughput

Following notations are used to represent weighted user requirements and weighted WIDS metrics relationship.

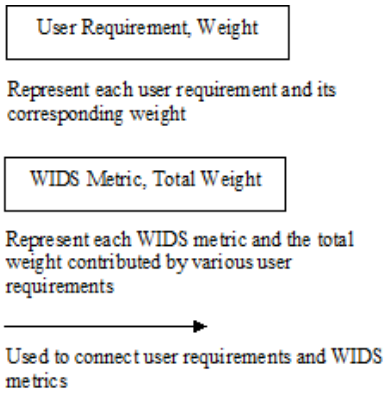

Figure 2: Notations used to represent user requirements and WIDS metrics relationship.

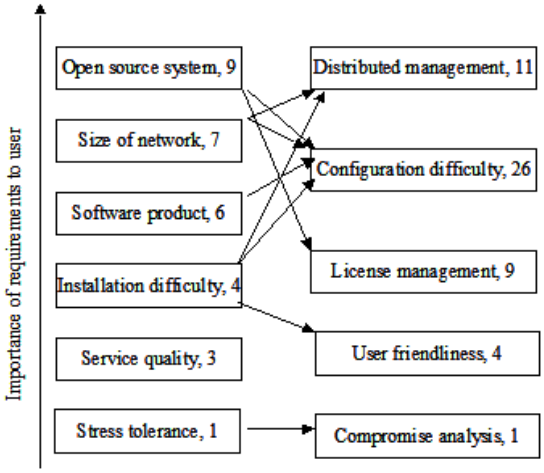

Figure 3: User requirement to WIDS metric weighting Example.

V. CONCLUSION AND FUTURE WORK

As a large number of WIDS products are available in the market, it becomes difficult for the user to select one of them that meet their requirements as these products differ in features and capabilities. In this paper we provide a user requirements weight based approach to be used for selecting a WIDS product. We describe various steps needed for the selection of WIDS product and how user requirements may be weighted. We also define various metrics concern with WIDS and how mapping of weighted user requirements to these metrics can be done. Although we tried our best to find out the user requirements and metrics concerned with WIDS, but a lot is to be done to find out more. The approach discussed in the paper may be extended by assigning negative and fraction weights to the user requirements so that more accurate selection of WIDS product can be done.

VI. REFERENCES

[1] Rupinder Singh, Dr. Jatinder Singh, A Metrics Based Approach to Intrusion Detection System Evaluation for Wireless Network, International Journal of Education and Applied Research (IJEAR) Vol. 1, Issue 1, Ver. 1: Jul. - Dec., 2011, ISSN : 2249-4944 (Print).
[2] Jeff Dixon, Wireless Intrusion Detection Systems Including Incident Response & Wireless Policy.
[3] Snehal Boob and Priyanka Jadhav, Wireless Intrusion Detection System, International Journal of Computer Applications (0975–8887) Volume 5– No.8, August 2010. http:// www.ijcaonline.org/volume5/number8/pxc3871312.pdf
[4] Gautam Singaraju, Lawrence Teo, and Yuliang Zheng1, A Testbed for Quantitative Assesment of Intrusion Detection Systems Using Fuzzy Logic, Proceedings of the Second IEEE International Information Assurance Workshop (IWIA'04) 0-7695-2117-7/04.
[5] Baiju Shah, How to Choose Intrusion Detection Solution, July 24, 2001 , Version 1.2e, Sans Institute infosec reading room.
[6] Dennis Mathew, Choosing an Intrusion Detection System that Best Suits your Organization, Sans Institute infosec reading room.

[7] Ruti Gafni, Framework for Quality Metrics in Mobile - Wireless Information Systems, Interdisciplinary Journal of Information, Knowledge, and Management Volume 3, 2008.
[8] Christos Xenakis a, Christoforos Panos b, and Ioannis Stavrakakis, A comparative evaluation of intrusion detection architectures for mobile ad hoc networks, 2010 Elsevier Ltd.
[9] Jacob W. Ulvila, John E. Gaffney, Jr., Evaluation of Intrusion Detection Systems, Journal of Research of the National Institute of Standards and Technology Volume 108, Number 6, November-December 2003.
[10] Lisa Phifer, Top Ten Wi-Fi Security Threats eSecurity Planet, March 08, 2010.
[11] Jeff Dixon, Wireless Intrusion Detection Systems Including Incident Response & Wireless Policy.
[12] Linda Westfall, 12 Steps to Useful Software Metrics, The Westfall Team.
[13] Cem Kaner and Walter P. Bond, Software Engineering Metrics: What Do They Measure and How Do We Know ?, 10th international software metrics symposium, metrics 2004.
[14] Marco Chiani, Andrea Giorgetti, Matteo Mazzotti, Riccardo Minutolo and Enrico Paolini, Target Detection Metrics and Tracking for UWB Radar Sensor Networks, ICUWB 2009 (September 9-11, 2009).
[15] Jatinder Singh, Dr. Lakhwinder Kaur, and Dr. Savita Gupta, Analysis of Intrusion Detection Tools for Wireless Local Area Networks, IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.7, July 2009.
[16] M. V. Ramana Murthy, P. Ram Kumar, E. Devender Rao, A C Sharma, S. Rajender, S. Rambabu, Performance of the Network Intrusion Detection Systems, IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.10, October 2009
[17] David J. Day and Benjamin M. Burns, A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engines, ICDS 2011 : The Fifth International Conference on Digital Society.
[18] Yousef farhaoui and ahmed asimi, "Performance method of assessment of the intrusion detection and prevention systems", yousef farhaoui et al. / international journal of engineering science and technology (ijest).
[19] Rupinder Singh, Dr. Jatinder Singh, "Logistic Metrics Scorecard Based Approach to Intrusion Detection System Evaluation for Wireless Network," IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501Vol.2, No.3, June 2012.
[20] Rupinder Singh, Dr. Jatinder Singh, "Architectural Metrics Scorecard Based Approach to Intrusion Detection System Evaluation for Wireless Network," Global Journal of Computer Science and Technology Network, Web & Security Volume 12 Issue 11 Version 1.0 June 2012.
[21] Rupinder Singh, Dr. Jatinder Singh, "A Performance Metrics Scorecard Based Approach to Intrusion Detection System evaluation for Wireless Network," Global Journal of Computer Science and Technology Network, Web & Security Volume 12 Issue 12 Version 1.0 Year 2012.