International Engineering Journal For Research & Development

Vol.4
Issue 5

E-ISSN NO:-2349-0721

Impact factor : 6.03

THE NEXT GEN INTRUCTION PREVENTION SYSTEM FOR WIRELESS LAN

S. V. Athawale
Computer Engg department , Aissm's , College of Engg
SPPU ,Pune, India
svathawale@gmail.com

Dr .M. A. Pund
Professor Department of Computer Science & Engineering,
PRMIT & R, Badnera – Amravati,
Indiapundmukesh@gmail.com

Abstract-

Now a day a rapid and instant growth of WLAN, wireless intrusion prevention systems have lately become the researcher hotspot. In this paper, we first examine the drawbacks of WLAN and point out the prime 802.11- definite threats, then present the wireless IPS with an intelligent pre-decision engine using mobile agent technology, specially demonstrate the need for mobile agent detection in WLAN. By importing a supporting degree of intrusion plan, this engine can predict and avoid the future attacks and directly respond to these actions. We propose an improved model for conducting attack recognition and making pre-decision. Experimental results showed that the mobile agent detection and predecision engine can not only improve detection but also the prevention performance and most reduce false positives evidently in WLAN.

Keywords— Wireless LAN, Intrusion Prevention System, 802.11 WLAN, Threats, Attacks.

INTRODUCTION

The meager cost of wireless networks and relative ease of use, cause organizations to invest in wireless networks as conflicted to traditional LANs. Although so many attempts have been made to secure these networks, the technology is still highly vulnerable and susceptible to active and passive intrusions. Security methods like cryptography and firewalls do not satisfy user's needs. This causes the requirement and use of more complex security systems, such as Intrusion Detection Systems (IDSes). Due to the long history of wired LANs, so many IDSes have been developed.

Although the traditional wired IDSes are powerful systems, unfortunately they do little for the wireless world. Modelling normal behaviour of a system, in anomaly IDSes, is so bulky due to its complexity. But in other hand, they are best for detecting new attacks. Due to the predefined pattern of previous attacks, misuse IDSes are vulnerable to future ones. Hybrid IDSes takes assets of two preceding systems to resolve their deficiencies. In this paper we present hybrid wireless-IDS.

The firewall isn't like the network IPS -- it's not a must-have security device found in most every enterprise network. Even so, today's intrusion prevention system is still gaining new infrastructure.

The IPS is sharing major traffic attack data with the firewall and gaining virtualization features, horsepower, and enhancements to become more application-aware, as well as to help secure client machines. Compliance has helped keep the IPS mortal and well, despite predictions of its decease over the years. And it could be the federal government that gives IPSes a big boost: The intrusion detection system (IDS), which spits out event alarms but doesn't force on them like an IPS does, is still more likely to be sitting in an enterprise.

IDS/IPS LITRATURE SURVEY

Related work

There have been other many researcher work on intrusion detection and prevention system their major contribution are in [1] they were demonstrated result better intrusion prevention system in the indoor environment , in the era of wireless the rapid growth and the road map of next generation intrusion detection and prevention system guideline and proposed model was explain in [2]. In this they optimally choose wireless access point [3], they also demonstrated better algorithms to increase in indoor positioning accuracy. In this they proposed experimentally [4] shown high detection rate and high prevention rate with low vulnerability.[5] In this they were discuss the detail about wireless node and its implementation and verify the feasibility of the system. In [6] they introduce the solution and light weight for the betterment of cryptographic primitive. They [7] in this they were

not only reflects the non-inclusive among evidences, and then, this paper gives the process of combination rule of the new method typical examples showed the new method is effective and adaptability.

In [8] this paper they deal with modifying detection rule with simple method with network based intrusion detection system. This paper [9] they detect suspicious traffic and generate network alert. In this multi level IDS/IPS for both incoming and outgoing traffic. In this paper they were implemented Software Defined Network (SDN) and an enhance this to next level with open source software such as Suricata [10].In [11] this paper introduced network attacks and instruction detection/prevention system signature and anomaly based with data mining and machine learning approach. In this proposed [12] framework for IDS/IPS with data set to cover major areas of real world.

Background on IPS wireless Network

Securing computer systems and data on your computer have become very pivotal because of growing incidences of internet frauds, identity theft, spyware, viruses, cyberpunks and network attacks. All these elements have become such a real complication for almost every computer users. The level of security that system offers is not adequate because of the impulsive development of malicious and spiteful software's like Trojans, key loggers and root kits. The inadequacy inherent in current defenses has driven the development of a new breed of security products known as Intrusion Prevention Systems (IPS). An Intrusion Prevention System is a network device/software that goes deeper than a firewall to identify and block network threats by assessing each packet based on the network protocols in the network layer, the context of the communication and tracking of each session. IPS is a proactive defense mechanisms designed to detect malicious packets within normal network traffic and stop intrusions dead, blocking the offending traffic automatically before it does any damage rather than simply raising an alert as, or after, the malicious payload has been delivered. Intrusion prevention systems were invented independently by Jed Haile and Vern Paxon to resolve ambiguities in passive network monitoring by placing detection systems in-line on the network and if any bad traffic is detected, the same is dropped in real-time The network IPS isn't like the firewall -- it's not a must-have security device found in most every enterprise network. Even so, today's intrusion prevention system is still gaining new features and becoming more tightly integrated into the security infrastructure. The IPS is sharing more traffic attack data with the firewall and gaining virtualization features, horsepower, and enhancements to become more application-aware, as well as to help secure client machines. Compliance has helped keep the IPS alive and well, despite predictions of its demise over the years. IPS technologies are mostly session based and traffic flow is examined based on session flow. To cut a long story short, the most essential thing you should remember about system security is to start with prevention.

MATHAMATICAL MODELING

Let T represent a Height balanced tree that represents our proposed system for intrusion prevention system.

Let T = {E, V} where
E represents the set of edges; E = {e1, e2, e3 ....., e11} and
V is a set of vertices; V = {v0, v1, v2, v3....., v8}.

In the graphical representation of our proposed system, vertices in the set V represent the modules which are connected through directed edges in the set E representing the operation between the modules. The vertices are defined as follows,

VERTICES	MODULE
v1	Initialize
v2	Get packet
v3	Analyze packet by ping
v4	Scan IP, MAC, SSID
v5	Compare IP with database
v6	Compare MAC with database
v7	Compare SSID with database
v8	Notification to the admin
v9	Allow session
v10	Block session

The edges are defined as follows,

EDGE	OPERATION
e1	Use Jpcap to capture packets
e2	Analyze IP,MAC,SSID
e3	Call to database for checking IP
e4	Call to database for checking MAC
e5	Call to database for checking SSID
e6	Send notification
e7	Allow session if satisfied
e8	Admin takes decision
e9	Process continues

Let f_e be a rule of E * V such that for given edge; it returns vertices. f_e (E) |→ V.

Thus, for our proposed system,

$f_e(e1)$ = {*v2*}.....*v2 is called using e1 to capture packet.*

$f_e(e2)$ = {*v4*}.....*v4 is called using e2 to scan IP.*

$f_e(e3)$ = {*v5*}.....*v5 is called using e2 to scan MAC.*

$f_e(e4)$ = {*v9*}..... *v9 is called using e2 to scan SSID.*

$f_e(e5)$ = {*v6*}.....*call to database is made to check the obtained IP,MAC,SSID.*

$f_e(e6)$ = {*v7*}..... *a notification is sent to the admin.*

$f_e(e7)$ = {*v8*}..... *session if allowed if authorized by the admin.*

$f_e(e8)$ = {*v3*}..... *session is blocked*

$f_e(e9)$ = {*v10*}..... *to repeat the process for every new request.*

Complexity:

Our system involves four main modules

- Scan by IP
- Scan by MAC
- Scan by SSID
- Event selection

For a standard network scan and analysis module by using IP address, the complexity is logarithmic and it is given as

IP=O (log W)
Where
W=is the maximum length of a IP string.

For a standard network scan and analysis module by using MAC address, the complexity is logarithmic and it is given as
IP=O (log W)
Where W=is the maximum length of a IP string.

For a standard network scan and analysis module by using MAC address, the complexity is logarithmic and it is given as

MAC=O (log W)
Where
W=the length of an address.
n=the number of routing table entries.

For a standard network scan and analysis module by using SSID, the complexity is given as

SSID=O (n/k)
Where
n= is the number of strings.

W=is the maximum length of a string.

And the complexity of the event selection module depends on the number of events involved in it. Thus for n events, the complexity is
O (n).

Total Timing Complexity= IP Search Complexity + MAC Search Complexity + SSID Search Complexity + Event selection Complexity

= O (log W) + O (log W) + O (n/k) + O (n)
= **O (n)**
Thus our proposed system lies in P Class by Horner Rule.

Result

The main purpose of this study was to examine key attribute of traditional intrusion prevention system toward our next generation IPS application installation its approach. Table 1 presents the descriptive statistics of the contribution towards contribution of next gen IPS. When we using our approach administrator to control the information they would disclose and the information would to generalize, than when using the commonly used for next

Gen adopted approach In order to test our hypothesis, we conducted a repeated measures a-test, i.e. attacks test comparing the mean concern with information disclosure when using our approach to the mean concern with information disclosure when using the commonly adopted approach. The difference in

Fig. 1 Screenshot of the run application.

concern was statistically significant Number of beacon frames on all monitored channels per 50 seconds for twenty two computers, when using the commonly adopted approach. Hence, this result confirms our hypothesis, and proves that users are authentication concerned -as they should be- in disclosing significant amount of personal data to application developers. Moreover, we were interested in understanding the factors affecting next Gen approach. Specifically, we examined passive intrusion detection system and inline intrusion prevention system in Table 1. In other hand Table 2. Satisfies with our approach is order to cover various attacks over the wireless network in college proposed method attacks coverage shown in Table 2. That satisfied need of Next Gen IPS for WLAN when using our approach, its satisfied need of next Gen computing.

Table 1: DESCRIPTIVE STATISTICS OF NEXT GEN IPS

Key IPS Attribute	Typical IPS	Next Gen IPS for WLAN
Inline IPS & Passive IDS	✓	✓
	✓	✓
Default Detection Policies	✓	✓
Report, Alert & Dashboard	✓	✓
Customize Rule	×	✓
Vulnerability Based Protection	×	✓
Automated Assessment	×	✓
Automated Tuning	×	✓
User Identity Tracking	×	✓
Application Monitoring	×	✓
Network Behavior	×	✓
Virtual IPS & Management Console	×	✓

Table2: ATTACKS COVERAGE IN NEXT GEN IPS

Attacks Type	Typical WIPS	Proposed NGWIPS
Network Discovery	Only detected	Prevented
Eavesdropping	Not detected	Prevented
Impersonation	Only detected	Prevented
n-in-Middle	Only detected	Prevented
Denial of Service	Only detected	Prevented

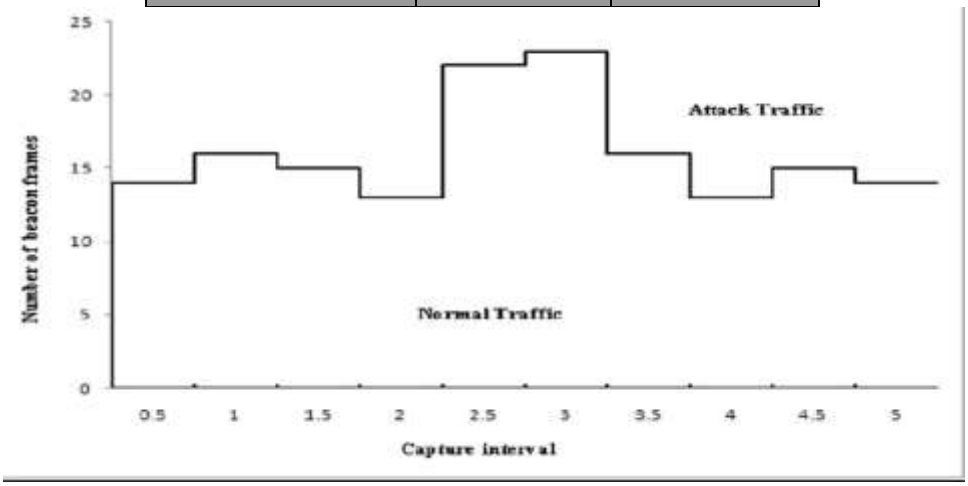

Fig. 2. Number of beacon frames on all monitored channels per 50 seconds

CONCLUSIONS AND FUTURE DIRECTION

In this paper we have presented next generation intrusion prevention system in wireless LAN applications that enables user to specify profile attribute preferences and requires applications to be designed so to be customized based on users profile preferences. Our IPS framework provided privacy- enabled solution that is inline solution with strong authentication in order to achieve high accuracy and security system and it require very less time over the wireless network. We modelled the applications as finite state machine with transition labelling indicating the generalization level required to enable application state transitions it is mathematical modelling in order to find completeness of system our system is NP complete. Additionally, we assessed the user's perceived benefits and

the ease of use of this type of approach by conducting a user study. As presented in the paper, the results are very much positive; users acknowledge that these types of solutions are needed and that our approach would allow them to enjoy more confidently the functionalities offered by various applications levels. The traditional IPS uses the old technique of Centralized RF Scanning, SSID scanning, hence generating lots of Network Traffic. Also the previous techniques are unable to detect the intrusions which use internal compromised proxies to hide themselves. Our system takes advantage of Divide and Conquer algorithm hence making our system more efficient. The model makes it easier to implement well organized network management system. It can satisfy the need of future computing. In the future, we plan to investigate the current work along several directions. First, we plan on extending the functionalities of the traditional technique, to support inline and customized generalization values. We will explore whether on topologies can be integrated with the social network system, so as to support a large variety of generalized values. Digital Certificates to provide higher security in wireless networks. Providing support for different operating systems. Automation of the system by minimizing the interference of the administrator.

ACKNOWLEDGMENT

We will like Thank all research community who had inspire us to work on such wonderful topic. The authors also thank to the anonymous referees for valuable comments.

REFERENCES

Iyad H Alshami , Noor Azurati Ahmad , Shamsul Sahibuddin, "People effects on WLAN-Based IPS" accuracy experimental preliminary results
," IEEE Confrance , pp. 206-209, Sept 2014.

M. A. Pund , S. V. Athawale,"NGIPS: The road map of next generation intrusion prevention system for wireless LAN," IEEE Conferance, pp. 276-280, October 2017.

Bang Wu , Zixiang Ma , Stefan Poslad , Wei Zhang,"An efficient wireless access point selection algorithm for location determination based on RSSI interval overlap degree determination," IEEE Conferance. , pp. 1-8, April 2018.

Nen-Fu Huang , et al,"An OpenFlow-based collaborative intrusion prevention system for cloud networking," IEEE Conferance, pp. 85–92, June 2015.

Yao Hui Wang, Zheng Xiang Li,"Design of Wireless Node Based on AR9341," Procedia Computer Science, Vol. 154, 2019, pp. 416-423, 2019.

Younes Asimi, Ahmed Asimi, et al., "Unpredictable cryptographic primitives for the Robust Wireless Network Security," Procedia Computer Science, Vol.134, pp. 316-321, 2018.

Xu-Hui Lan, Ling-Zhi Li, Yong-Min Guo, Chang-Xi Li, "A New Combination Rule of Evidence Theory on Multi-Source Information Fusion," ACM Proceedings of the 2017 International Conference on Wireless Communications, Networking and Applications., pp. 235-239, October 2017.

Krakow, Poland,"Mining intrusion detection rules with longest increasing subsequences of q-grams," ACM Proceedings of the International Conference on Research in Adaptive and Convergent Systems ,pp. 25-29 20, September 2017.

Atul Sawant,"A Comparative Study of Different Intrusion Prevention Systems," IEEE Fourth International Conference on Computing Communication Control and Automation (ICCUBEA),pp.1-5,Auguest 2018.

Kiho Nam,Keecheon Kim,"A Study on SDN security enhancement using open source IDS/IPS Suricata," IEEE. Conferance., pp. 1124-1126, Octmber 2018.

Lidong Wang ,"Big Data in Intrusion Detection Systems and Intrusion Prevention Systems," sciepub Journal of Computer Networks, pp.48-55, August 2017.

Iman Sharafaldin, Amirhossein Gharib, Arash Habibi Lashkari and Ali A," GhorbaniTowards a Reliable Intrusion Detection Benchmark Dataset," Vol: 2017 Issue: 1, pp. 177-200 ,January 2018.