www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 11 Nov. 2016, Page No. 19116-19118

A New Improve Intrusion Prevention System Security for Wireless LAN A Review

K K. Mahurkar, S V. Athawale
M.E. Computer Engineering,
Department Of Computer Engineering All India Shri Shivaji
Memorial Society's College Of Engineering
Pune, India
Asst. Professor, Department Of Computer Engineering All India Shri Shivaji
Memorial Society's College Of Engineering
Pune, India

Abstract- Threat in any system can be identified only when we have full knowledge of the system. And threats can also be prevented if proper tools or mechanisms are present or developed. So, this paper review not only identifies the problem in Wireless LAN but also reviews previously proposed solutions to the threats that exploit communication through WLAN. And presents new prevention mechanism to the existing problem with securing its main server. The paper reviews the experiments conducted to study the impact of various attacks on the system and also post solution results evaluation. A hybrid approach is used for deep packet inspection over network traffic to resolve unauthorized access in WLAN, provide satisfactory results in performance.

Keywords: WLAN: Network, Wireless Local Area Network, IPS: Intrusion Prevention System, Agent Based System, hybrid approach.

1. INTRODUCTION

WLAN has blended so well with the existing network environment such that in every corner of Railway Station, Industries, Residential Areas, Institutions and much more; its relevance is out of the question. It is better than Wired Connection is many aspects as physical resource requirements gets less, which also impacts is reduced network cost, etc. The Wireless LAN or WLAN got its spike as soon as it touched the network environment. Behaving as the easiest way to plug and play media for the internet and other important capabilities. Besides earning reputation and giving more functionality than wired LAN, it blinded many consumers about the security threat that WLAN capable of bringing with it. Discovered in the early 90s were the same threat as wired had to face like Denial of Service Attack, Man in the Middle Attack and much more. Also, some new attacks got introduced in the emergence of WLAN such as Network discovery attacks, Eavesdropping/Traffic analysis, etc. Several popular works have also been done to eliminate or identify and prevent these attacks such as Wireless Intrusion Detection System (WIDS) [3], and various policies optimizer algorithms emerged for proper communication in WLAN. In the following parts, we will discuss Intrusion Detection System, after which a detailed Literature Survey, which would give the idea of related work already done their advantages or disadvantages. So as to determine the relevance for this review. Furthermore, we will go through the Propose Idea and Results and its relevance. Following with Conclusion.

2. INTRUSION PREVENTION SYSTEM

Detection can done after a certain attack has taken place. And prevention is meant to take measures so that attack does not happen. This small difference is likely to misunderstand by anyone so the clarity of the two must do. We can do the any of the things like firstly doing detection from other sources. And the creating a prevention system by analyzing the detected attacks. So, the traditional prevention system can only detect and respond to the destruction of the system. And Nowadays, Intrusion Prevention System have been used in WLAN, to monitor and analyze unauthorized user activities, determine the kind of intrusion, detect illegal network behavior, and give an alert for abnormal network behavior for preventing attacks in WLAN. The only key points to remember while designing Intrusion Prevention System are of change coverage and latency in the network. Upgrading all traditional Intrusion Prevention System with Machine Learning Algorithms capability is another approach for better detection and also prevention of attacks in WLAN.

3. RELATED WORK

The work on WLAN is not new and many Intrusion Prevention System are already in existent with proper theory and real-time usage. We will be discussing the various impact on the WLAN through a study conducted and their relevance. [1]The Author Alexandros Tsakountakis et. el. worked on "Towards effective Wireless Intrusion Detection in IEEE 802.11i" in the year 2007. They studied various attacks in WLAN like Network discovery attacks, Eavesdropping/ Traffic analysis, Masquerading /Impersonification attacks, Man-In-The-Middle (MITM) attacks, Denial-of-Service (DoS) attacks, and also special attacks that can probably happen in IEEE 802.11i called IEEE 802.11i specific attacks. Also discovered various algorithms or steps to prevent such attacks like detection of Netstumbler, Detection of De-authentication flood and others. Their study determined that major concern lies on DoS attacks and also introduced WIDS. The advantages of this paper are a detailed study of attacks and also various solutions which could be applied to the attacks. The only disadvantage in this paper is that it does not cover the centralised and distributed WLAN which in turn brings other security concerns.[2] Author Xiao Qiang Peng et. el. published a paper titled as "The intrusion detection system design in WLAN based on Rouge AP" in 2010. Xiao et. el. gave emphasis on WIDS and the proposed the application of strong security policy on WIDS can secure WLAN. Describing rough as illegal or unauthorised access Xiao et. et. Concluded that only single technology cannot solve the security problem, so as to create a multilevel security architecture. [3] Auther Huan-Rong Tang et. el. in 2009 presented paper titled as "WIRELESS INTRUSION DETECTION FOR DEFENDING AGAINST TCP SYN FLOODING ATTACK AND MAN-IN-MIDDLE ATTACK" proposed a new architecture of WIDS for IEEE 802.11 wireless infrastructure networks, where the WIDS detects man-in-the-middle attack by analyzing the channel gap. And secures from other existing attacks. Huan et. el. conclude by showing experiments about more precise architecture to detect rough AP. But limits itself by proposing that Machine Learning could help in delivering more accuracy. This paper actually takes WIDS one-step further than [2] and improves accuracy but concerns its ideas for security concerns in centralized systems which may benefit it. [4]Author Debabrata Nayak who is Member of IEEE, published a paper titled "An Adaptive and Optimized Security Policy Manager for Wireless Networks" in 2007. In this paper, unlike others, author Nayak presented a detailed study on the Policies which must be considered in Wireless Network. Also, Nayak helped in understanding the disadvantages of Centralized depository which caused a bottleneck in any dynamic network. This bottleneck was removed using Security Policy Optimiser Algorithm.But did not included the RAID technology so as to improve the centralized part further [5] Authors Yaqing Zhang et. el. presented a paper titled as "Client-based Intrusion Prevention System for 802.11 Wireless LANs" a true motivation for our hybrid architecture. Zang et. el. presented a client-based scheme such that by using MAC filtering mechanism the client will be able to differentiate between legitimate and forged management frames. Their mechanism is non-cryptographic and hence delivers high performance and low-level latency. They introduced adaptive threshold algorithm which determined a time complexity of O (1) giving maximum performance. The only limitation is that their system uses distributed environment which decreases the scalability factor. So as proposed in this review a centralized approach with RAID technology can help in determining the efficiency and increase in performance too.[14] Glenn C. Langford, presented "Centralized secure backup system and method" in which author presented his idea of backing up centralized system for which he used encryption and decryption policies with symmetric key mechanisms also cryptosystem. So this approach can be used in proposed system with [13].

4. PROPOSED SYSTEM OVER VIEW FOR IPS

New proposed system that uses Intrusion Prevention System is understandable and give proper and better results as compared to other approaches. This system is mainly with centralized server system with RAID technology or Centralized secure backup system [14], Also implementing the strong security policies [4]. Such that admin can evaluate due to agent based system and its reduced complexity maintains over time.

Case 1: Suppose attacker tries to connect his laptop or mobile device directly to wireless .And if it is not in database then attacker cannot connect to it.

Case 2: If someone who is already inside in the network wants to do unauthorized activity .Then runtime prevention systems is run which verifies MAC, SSID and IP along with unique ID.

Case 3: In some cases attackers want to connect with help of software. Then we just trap with unique network ID, which manages my centralized server system.

Case 4: Suppose intruder tries to get into the system by any unauthorized policies then a secured encryption and decryption method will protect the centralized system from doing so.

Case 5: If we consider that somehow our centralized system gets destroyed or sleeps when it is most probably needed, then we use RAID disk for the backups too.

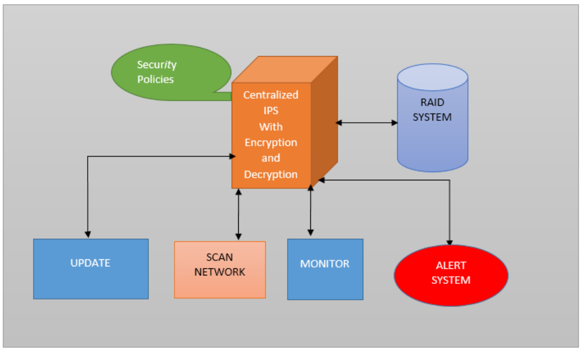

Figure1. Hybrid Architecture of WLAN

5. CONCLUSION

In this paper, we have presented new agent based communication over wireless along with the centralized server which improved performance, security and backup such that improving the security mechanisms by implementing security policies and RAID system. Centralized server makes the system more stronger security on wireless network. But only by giving centralized server the answer to every attack is not possible and also not feasible. Many new trends such as Internet of things, Cloud Computing, Big Data impose more threats for security, migration of dat. This in turn increases the work of Intrusion Prevention System which must cope with efficient method are required to reduce network overhead associated with this method.

6. REFERENCES

[1] Alexandros Tsakountakis, Georgios Kambourakis and Stefanos Gritzalis, 2007.*Towards effective Wireless Intrusion Detection in IEEE 802.11i.*

[2] Xiao qiang Peng,Cheng Zhang, Dian gang Wang, 2010.*The intrusion Detection System design in WLAN based on Rogue AP*.

[3] Huan—Rong Tang, Rou-Ling Sun, Wel-Qiang Kong,2009.*Wireless Intrusion Detection For Defending Agaunst TCP SYN FLOODING ATTACK AND MANIN-THE-MIDDLE ATTACK.*

[4] Debabrata Nayak, 2007.*An Adaptive and Optimized Security Policy Manager for Wireless Networks.*

[5] Yaqing Zhang,Srinivas ,2010.*Client-based Intrusion Prevention System for Wireless LANs 802.11.*

[6] Khalil El-Khatib, 2010.*Impact of Feature Reduction on the Efficiency of Wireless Intrusion Detection Systems.*

[7] Samer Fayssal,Byoung Uk Kim,2010.*Performance Analysis Toolset for Wireless Intrusion Detection Systems.*

[8] Sunghyuck Hong,Sunho Lim,2010.*Analysis of Attack Models via Unified Modeling Language in Wireless Sensor Networks: A Survey Study*.

[9] Shanshan Jiang and Yuan Xue, 2009.*Optimal Wireless Network Restoration Under Jamming Attack.*

[10] Ritu Chadha, Hong Cheng, Yuu-Heng Cheng, Jason Chiang, 2004.*Policy-Based Mobile Ad Hoc Network Management**.

[11] Hua Li, Dimitri Reizvikh and Lucy (Liang) Lei,2007.*An Improved Defense Scheme Against Attacks On Wireless Security*.

[12] Larry Korba, 1998.*Security System for reless Local Area Networks*.

[13] Peter M. Chen, 1994. *RAID: High-Performance, Reliable Secondary Storage*.

[14] Glenn C. Langford, 1999. *Centralized secure backup system and method*.