International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:5, No:5, 2011

Key Issues and Challenges of Intrusion Detection and Prevention System: Developing Proactive Protection in Wireless Network Environment

M. Salman, B. Budiardjo, K. Ramli

***Abstract*—**Nowadays wireless technology plays an important role in public and personal communication. However, the growth of wireless networking has confused the traditional boundaries between trusted and untrusted networks. Wireless networks are subject to a variety of threats and attacks at present. An attacker has the ability to listen to all network traffic which becoming a potential intrusion. Intrusion of any kind may lead to a chaotic condition. In addition, improperly configured access points also contribute the risk to wireless network. To overcome this issue, a security solution that includes an intrusion detection and prevention system need to be implemented. In this paper, first the security drawbacks of wireless network will be analyzed then investigate the characteristics and also the limitations on current wireless intrusion detection and prevention system. Finally, the requirement of next wireless intrusion prevention system will be identified including some key issues which should be focused on in the future to overcomes those limitations.

***Keywords*—**intrusion detection, intrusion prevention, wireless networks, proactive protection

I. Introduction

THE growth of wireless networking has confused the traditional boundaries between trusted and untrusted networks. Wireless Networks are subject to a variety of threats and attacks at present [6]. First, wireless technology provides a convenient way of connecting various computers to a network with radio waves. In wireless network, the clear border of defense does not exist and the attack may come from all potential places. So at any time any nodes such as Access Points (AP) or client stations may be the victims. Second, an attacker using the wireless card and WiFi detection tool can easily find any access point right around. For example, war-driving using NetStumbler or Kismet will present attackers with the detailed wireless information, such as the identification, channel, and encryption method [7].

M. Salman is with the Department of Electrical Engineering, Faculty of Engineering, University of Indonesia (phone: +62-21-7270078; fax: +62-21-7270077; e-mail: salman@eng.ui.ac.id).

B. Budiardjo is with the Department of Electrical Engineering, Faculty of Engineering, University of Indonesia (phone: +62-21-7270078; fax: +62-21-7270077; e-mail: bbudi@eng.ui.ac.id).

K.Ramli is with the Department of Electrical Engineering, Faculty of Engineering, University of Indonesia (phone: +62-21-7270078; fax: +62-21-7270077; e-mail: k.ramli@eng.ui.ac.id).

The information can help attackers try to exploit a wireless target. Third, the present 802.11 WLAN encryption methods including WEP, WPA and WPA2 are all weak and insufficient [25]. Research has indicated that 128-bit WEP key of a wireless transmission can be quickly decrypted via BackTrack or Aircrack-ng tool. Even an attacker can potentially decrypt the WPA/WPA2 key using Cowpatty tool [22]. Fourth, wireless networks are subject to DoS (Denial of Service) attack. Attackers can launch malicious DoS attacks by authentication flood, deauthentication flood, association flood, disassociation flood and so on. These attacks are so effective that the wireless target network will be unable to serve its legitimate users. Last, hackers can attack wireless networks via MITM (Man in the Middle). By introducing an unauthorized *(rogue)* Acess Point (AP) into the wireless networks, the hacker can gather sensitive packets in the communication process. Most wireless clients simply connect to the AP with the best signal strength, so once the victim is associated to those kind of AP, all packets can be captured. The hacker can analyze some valuable information such as user account and plain password. This situation will lead to a chaotic wireless network environment. Intrusion Detection and Prevention Systems are considered to be an important solution to solve this problem. But now, it has a serious problems since it is difficult to manage and maintain the intrusion signatures and databases, it requires a lot of time and effort in order to maintain the sensor security policy updates.

The aim of this paper is to analyze the drawbacks of wireless networks and indicate the primary threats, then investigate the characteristics and also limitations on current wireless intrusion detection and prevention system. Finally, the requirement of next wireless intrusion prevention system will be identified including some key issues which should be focused on in the future to overcomes those limitations.

II. Threat To Wireless Network

Risks identified from the use of Wireless Networks have shown that the five aims of security, confidentiality, integrity, availability, authenticity and non-repudiation cannot be met [14]. The comparison of security threat between Ethernet (wired) and Wireless Networks is shown in table 1:

In term of the encryption method, a major weakness with WEP was documented in the Fluhrer, Mantin and Shamir paper "Weaknesses in the Key Scheduling Algorithm of RC-4." This weakness deals with a flaw in the RC-4 implementation that allows a passive user to sniff wireless traffic and brute force the WEP key in a short period of time [9]. Two tools of choice that automate this attack are WEPCrack (http://wepcrack.sourceforge.net/) and Airsnort

TABLE I
SECURITY THREAT: ETHERNET VS 802.11 WIRELESS NETWORK[17]

Security Threat	Wired (Ethernet)	Wireless (802.11)
1. High potential for eavesdropping	-	√
2. High potential for DoS attack	-	√
3. Intrusion: Vulnerable to network layer (and above) attacks	√	√
4. Intrusion: Vulnerable to MAC/PHY layer attacks	-	√

(http://airsnort.shmoo.com/). Regardless of the key strength, these tools make the task of sniffing and using brute force to recover a WEP key become trivial. Once an attacker is in possession of a WEP key, he will be provided access to the WAP and anything to which it is connected.

Another common attack is Media Access Control (MAC) address masquerading. In this attack, malicious wireless users sniff traffic to determine MAC addresses that are being allowed access to a wireless network. Since most WAPs allow for this primitive type of authentication, once the attacker uncovers a validated MAC address, he can simply change his own MAC address using ifconfig under Linux or Control Manager under Microsoft® Windows® to change his MAC to that of the validated user. The attacker can then receive access to a WAP that is only concerned with authenticating MAC addresses. This attack only requires a wireless sniffer such as Airsnort. Because of the simplicity to circumvent, MAC-based authentication is never suggested.

Another attack and possibly one of the most serious types is AP masquerading, often called man-in-the-middle attack. In this attack, a malicious user sets himself up to be an *(unauthorized)* access point. Users authenticate to him instead of to the appropriate *(authorized)* access point, so the attacker now has complete control of their communications not to mention authentication information later required for access to authorized APs. Tools such as FakeAP (http:// www.blackalchemy.to/project/fakeap/) provide an automated method of setting up such APs and are advanced enough to alter transmit signal strength and MAC addresses to make numerous APs appear valid.

Finally, improperly configured access points provide the greatest risk to a wireless networks. This situation will allow an attacker to essentially walk into an internal network much like an open, unlocked door allows anyone to walk into an office undetected. This example points out the continuing importance of the biggest risk to security due to the expose of data structure stored with the link of wireless APs. The information includes an AP's SSID, MAC address, channel, channel, encryption, signal strength, type and so on as shown in Fig 1.

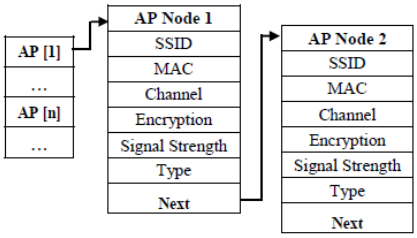

Fig. 1 Data structure stored in wireless APs [10]

III. WIRELESS INTRUSION DETECTION AND PREVENTION

An intrusion detection and prevention system (IDPS) is a network security device that monitors network activities for malicious or unwanted behavior and can react to block or prevent those activities in real-time. It improves network security by integrating the advantages of firewall and IDS *(Intrusion Detection System)* properly. An IDPS combines the blocking capabilities of a firewall with the deep packet inspection of an IDS. A variety of intrusion detection and prevention systems (IDPS) are well applied in wired network, but there are some difficulties to develop and implement a wireless IDPS. Unlike wired security devices, wireless IDPS must monitor the airwaves to detect wireless threats and make active response. Under wireless conditions, IDPS should provide particular wireless-specific network threat detection and mitigation against malicious attacks. A common framework for wireless intrusion detection and prevention is shown in Fig 2.

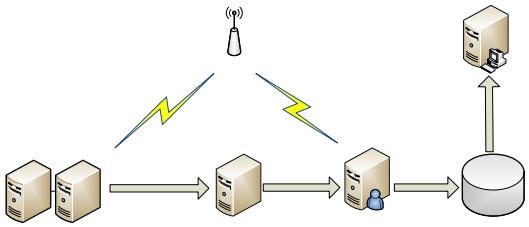

Fig. 2 Common wireless intrusion detection and prevention framework [15]

An excellent wireless IDPS must have the following basic functions [20]:

- Automatic detection and classification of wireless network threats.
- Accurate plan recognition of continuing attacks by hackers.
- Active response and prevention of the attack behavior that has happened, is happening or will happen.

Although the advantages of IDPS are obvious, it needs to consider the system performance since it will increase the

network load, resulting in data transmission delay. In order to avoid a system performance bottleneck, IDPS must have a wire-speed data processing ability to provide the second layer and third layer of switches, the same processing rate. Second, it also needs to consider security, should be as much as possible to filter out malicious attacks, making the IDPS is also facing an issue of misinformation and omissions. In improving the accuracy, IDPS face greater pressure. Once it makes a wrong decision, it will miss the true attack transactions. In the IDPS there are still some other drawbacks [15], such as:

A. Lack of standard wireless architecture

Inspite of current wireless IDPS can prevent some attacks in wireless networks, it cannot provide advanced architecture. It is different from a wired IPS whose location of detectors follows the logical structure of the network, detectors of wireless IDPS have to be placed based on physical location. So it makes sense to provide a standard architecture to make the implementation will be more easily.

B. Less Accurate with high rate of false positives

All real time IDPS system can suffer from issuing false alarms. Once instrusion is detected, wireless IDPS will abandon the data packets, which will form another type of denial of service. This leads to improperly reaction in facing the attack.

C. Insufficient update of attack signatures

An attacker usually at first, need to collect as much as data traffic before attempting an intrusion. This type of passive sniffing is quite dangerous, but there is nothing to do in this direction except to use the proper protection through encryption [6]. In addition, the IDPS has a drawback since it only keeps signature files based on known attack pattern recognition files given to them. It only has protection against what are known to be attacks. It does not have sufficient intelligence to recognize all the attacks against the database application, and establishing its update agressively.

IV. Related Works

Actually, there have been some researches on wireless intrusion detection and prevention system. However, there are some new challenges since it still have some limitations and drawbacks. It is, therefore, not surprising that there are already some researchers or engineers would like to continue working on it. Although it is still in starting stage, it has been some research achievements. Wen-Chuan Hsieh etc. (2004) proposed a Proactive Wireless Intrusion Detection System, which is capable of preventing common wireless attacks such as WEP cracking, MAC address spoofing and war-driving, by utilizing Short Message Service (SMS) and proactive techniques [23]. Dong Lijun etc. (2007) proposed a WTLS-Based Intrusion Prevention model, where a logical sole path is built between every wireless terminal and its destination, so an IPS engine can detect and prevent the traffics of user. Wireless Transport Layer Security (WTLS) is introduced firstly and then, they explore a solution of WIPS [5]. Over-The-Air (OTA) prevention is one of the popular methods used in a WLPS. A. Vartak, S. Ahmad and K N Gopinath (2007) provided a test-bed based experimental evaluation of four Over-The-Air prevention techniques in mitigating unauthorized wireless communication. They also discussed the implications of experimental results on the design of WIPS [21]. Jack TIMOFTE (2008) described some WLAN networks security threats and their protection through wireless intrusion prevention systems [6]. Guanlin Chen, Hui Yao and Zebing Wang (2009) presented a framework of WIPS with an intelligent plan recognition and pre-decision engine using honeypot technology, which can predict the future attacks and directly respond to these actions. They also designed and implemented an improved model for conduction plan recognition and making pre-decision [11].

V. Future Works

Based on the investigation of the characteristics and also limitations on current wireless intrusion detection and prevention system, there are some key issues which should be focused on in the future to overcomes those limitations:

A. Proactive and real-time prevention

The IDPS shoud provide a real-time attack prevention and analysis, can be in any unauthorized activity before the start of an attack, and prevent it from access to important resources.

B. Seamless Protection and Location Anonymity

Since the average user is not very familiar with the higher-layer security mechanisms. It needs to have a mechanism in hiding the access point and location identification as a way to protect the wirelss network against unknown intrusion and potentially malicious users.

C. The low rate of False Positives

Current IDPS still suffers from issuing false alarms. This leads to improperly reaction in facing the attack. It needs to have a better and more accurate in identifying the intrusion in real time to reduce significantly its false positives by implementing a self-defending network mechanism.

VI. Conclusion

In this paper, the threats to wireless networks are identified, then introduce an overview of intrusion detection and prevention system in wireless networks, and also investigate its limitations. Wireless networks are subject to a variety of threats and attacks at present. An attacker has the ability to listen to all network traffic which becoming a potential intrusion. Intrusion of any kind may lead to a chaotic condition. To overcome this issue, a security solution that includes an enhanced intrusion detection and prevention system need to be implemented. In future work we are interested in more advanced system of the wireless IDPS. Enhancing its detection and prevention approach in facing more sophisticated wireless attacks. There are some key issues which should be focused on in the future to overcomes those limitations with Proactive and real-time prevention of attacks;

Seamless Protection, Location Privacy and Anonymity and low rate of false positives.

REFERENCES

[1] Aleksandar Lazarevic, Vipin Kumar, Jaideep Srivastava, "INTRUSION DETECTION: A SURVEY", Managing Cyber Threats: Issues, Approaches and Challenges, Vol. 5, 2005, Springer Publisher.
[2] Alina Olteanu and Yang Xiao, "Security Overhead and Performance for Aggregation with Fragment Retransmission (AFR) in Very High-Speed Wireless 802.11 LANs", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 9, NO. 1, JANUARY 2010
[3] Alvaro A.Cardenas, "A Framework for the Evaluation of Intrusion Detection Systems", IEEE Symposium on Security and Privacy, 2006
[4] Carl Endorf, "Intrusion Detection and Prevention", McGraw-Hill/Osborne, 2004
[5] Dong Lijun, Yu Shengsheng, Xia Tao, Liao Rongtao. "WBIPS: A Lightweight WTLS-Based Intrusion Prevention Scheme", In Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing, IEEE Press, Sept. 2007, pp. 2298-2301.
[6] Earle, A.E., "Wireless Security Handbook", Auerbach Publications Taylor & Francis Group, New York, 2006
[7] Fernandez, E.B., Jawhar, I.. Petrrie. VanHilst, M., "An overview of the security wireless network", http://csrc. nist.gov/publications/ nistpubs/80048/NIST_SP_800-48.pdf, 2004
[8] Gast, Matthew, "802.11Wireless Networks: The Definitive Guide", Sebastopol,CA: O'Reilly, 2005
[9] Gunter Schafer, "Security in Fixed and Wireless Networks: an Introduction to Securing Data Communications", Wiley, 2003
[10] Guanlin Chen1, Hui Yao, Zebing Wang, "An Intelligent WLAN Intrusion Prevention System Based on Signature Detection and Plan Recognition", Second International Conference on Future Networks, 2010
[11] Guanlin Chen, Hui Yao, Zebing Wang, "Research of Wireless Intrusion Prevention Systems based on Plan Recognition and Honeypot", In Proceedings of the International Conference on Wireless Communications & Signal Processing, IEEE Computer Society, Nov. 2009
Jack TIMOFTE, "Wireless Intrusion Prevention System", Revista Informatica Economica, vol. 47, March 2008
[12] Lane, Heater D.. Securities Vulnerabilities and Wireless LAN Technology. SANS Institute, Virginia Beach 2006.
[13] Lynn Michael T., Hrastar Scott, "Method and system for actively defending a wireless LAN against attacks", United States Patent Application 20030233567, Jun. 2002
[14] Manivannan, N. dan Neelameham, P., 2006, "Wireless Security Techniques", Georgian Electronic Scientific Journal: Computer Science and Telecommunications 2006 No.2(9)
[15] Paul Bedell, "Wireless Crash Course", 2nd Edition, McGraw-Hill, 2005
[16] Paul DeBeasi, "802.11n: The End of Ethernet?", Network and Telecom Strategies In-Depth Research Report, Burton Group Sep 14, 2009
[17] Timothy D. Wickham, "Intrusion detection is dead. Long live prevention!"http://www.sans.org/readingJoom/whitepapers/detection/ 1028.php, 2003.
[18] Timothy R.Schmoyer, "Wireless Intrusion Detection and Response: A Case Study using the Classic Man-in-the-Middle-Attack", IEEE Communication Society, 2004
[19] Tung, S.S, Ahmad, N.N., Geok, T.K., 2006, "Wireless LAN Security: Securing Your Access point", IJCSNS International Journal of Computer Science and Network Security", VOL.6 No.5B, May 2006
[20] V. Vartak, S. Ahmad, K N Gopinath. "An Experimental Evaluation of Over-The-Air (OTA) Wireless Intrusion Prevention Techniques", In Proceedings of the 2nd International Conference on Communication Systems Software and Middleware, IEEE Computer Society, Jan. 2007, pp. 1-7.
[21] Vladimirov, Andrew A., Konstantin V. Gavrilenko, and Andrei A. Mikhailovsky. "Wi-Foo: The Secrets of Wireless Hacking", Boston: Addison-Wesley, (2004)
[22] Wen-Chuan Hsieh, Chi-Chun Lo, Jing-Chi Lee, and Li-Tsung Huang, 'The implementation of a proactive wireless intrusion detection system", In Proceedings of the Fourth International Conference on Computer and Information Technology, IEEE Press, Sept. 2004, pp. 581-586.
[23] Wu Junqi, "Study of Intrusion Detection System (IDSs) in Network Security", IEEE Wireless Communication, 2008
[24] Yujia Zhang, Guanlin Chen*, Wenyong Weng, Zebing Wang, "An Overview of Wireless Intrusion Prevention Systems", 2010 Second International Conference on Communication Systems, Networks and Applications
[25] Yaqing Zhang, Srinivas Sampalli, "Networking and Communications Client-based Intrusion Prevention System for 802.11 Wireless LANs", 2010 IEEE 6th Intemational Conference on Wireless and Mobile Computing.