IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

Intrusion Prevention System for Wireless LAN Security: A Study

S V Athawale[1], M A Pund[2]

Research Scholar, Computer Engineering Department, Sant Gadge Baba Amravati University, Amravati, India [1]

Professor, Department of Computer Science & Engineering, PRMIT & R, College, Badnera-Amravati , India [2]

Abstract: The security of wireless LAN networks is a talented topic which in current years has been the focus of much interest in the research community. Even as many security issues in these wireless networks can be addressed by etiquette design, wireless nodes have intrinsic much physical vulnerability that can be exploited by attackers to origin disruptions in network traffic. The scenery of these exposures is such that there is little that can be done to eliminate them leaving the network. It is vital that the impact of such attacks is well-understood before IPS for wireless ad hoc networks are used in mission-critical application. This paper is a stride in this threat analysis as our effects of attacks that exploit physical susceptibilities. Our contributions in this paper are, we combine risk and vulnerability characterizes them so that we understand various attack and their attack scenarios. We present study of various attacks along with attack scenarios in the context of a wireless LAN security.

Keywords: Vulnerability, LAN, IPS, Exploit, Attacks

INTRODUCTION

Enterprise wireless LANs have evolved into critical network communications, vital to every-day action. As a result, efficient wireless threat detection and prevention have become indispensible. However, unlike their wired counterparts, wireless networks are highly active, frequently changing in endpoint composition and location security. A moving target such as this requires a nimble defence that can immediately recognize and prevent new threats. But a static and increasingly stale Intrusion Prevention System (IPS) could leave otherwise secure WLAN vulnerable to emerging attacks and exploits for quite a long time. Updates like dynamic threat have long been a best practice in wired networks. In reality, very few establishments would consider a Unified Threat Management firewall or Network IPS appliance which lacked this agility.

To allow mission-critical wireless deployments while maintaining acceptable security posture, Wireless IPS (WIPS) must follow threads. Specifically, a robust WIPS must be elastic enough to incorporate dynamic updates whenever needed to mitigate zero-day threats. Introduction Enterprise wireless LANs have matured into critical network infrastructure, vital and important to day by day operation.

As an outcome, effective wireless threat detection and prevention have become indispensible. The term "wireless"reflect any means of communication that occurs without wires. Unguided media can be said as wireless, i.e. wireless is a way for transmitting electromagnetic effect but in unguided fashion. Wireless technology in simplest logic makes it able for one or more devices to communicate without any corporeal connection, without requiring network of peripheral wiring.

Wireless technologies have become increasingly popular in our everyday business and personal lives. The world of copper and fibber-based networks will continue to be the foundation of networks, but WI-FI is a rapidly emergent role. Wireless communication is a great magnetism to users who are continually on the move. Wireless network cards are installed on laptop computers rather than on desktop computers because of the inherent mobility that laptops bid. Wireless connectivity in PDA's and many other handheld computing devices is also getting popular. Getting right to the point, wireless technologies offer liberation and will undoubtedly continue to grow in popularity and increase performance efficiency .Over the past decade the price of wireless LAN equipments has dropped significantly. Wireless network card are nearing the price of their matching wired part. The performance improved spectacularly at the same time. In 1998 WLAN was at the top with 2 Mbps, now speed provided by WLAN is up to 100Mbps. This stupendous performance of wireless solution may lead to huge increase in the productivity by providing a real time access to E business applications and important network data. Communications maturity may be an initial reason for replacing the wired LAN with a wireless LAN. But increasingly the ease and elasticity and the ease of deploying WLAN s is appearing to enterprises.

Guanlin Chen, Hui Yao1, Zebing Wang. (2009) explain the WEP (Wired Equivalent Privacy) is weak; the standard 802.1x authentication method, WPA (Wi-Fi Protected Access) can also be decrypted using 4-way handshake packets to some extent. To aid in the detection and response of these potential threats, WLANs should supply a security solution that includes an intrusion prevention

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

system (IPS). They presented a wireless IPS with PRPE (Plan Recognition and Pre-decision Engine). This WIPS proposes the 802.11 packets-capturing model employing honey pot technique, expands the intrusion rules based on wireless device information, predicts the future actions of attackers using plan recognition, and finally offers the appropriate pre-decisions and responses to these malicious behaviours.

Jiqiang Zhai, Yining Xie (2011) studies highlighting Network Intrusion Prevention System with the basis of Windows, but most of the existing implementations of NIPS on Windows reappear to the third party firewalls lack of universality and portability. N. Wattanapongsakorn, S. Srakaew, C. Charnsripinyo (2012) they presents a network-based intrusion detection and prevention system (IDPS) which use machine learning algorithms to detect and classify network attacks.S.Vasanthi 1 and Dr. S.Chandrasekar.(2011) A network based Intrusion Prevention System ensconce in-line on the network, monitoring the incoming packets based on some prescribed rules and if any bad traffic is detected, the same is discarded in Real-time. They proposed new model which will combine the three techniques such as Adaptive weighted sampling algorithm, packets count flow classifier and Adaptive learning algorithms Guanlin Chen, Hui Yao, Zebing Wang (2009) Experimental results showed that the plan recognition and predecision engine can not only improve disclosure and prevention performance but also reduce false positives evidently. Ricardo Koller, Raju Rangaswami, Joseph Marrero, Igor Hernandez, Geoffrey Smith (2008) Intrusion detection and prevention systems must combat two challenges comprehensively performance and accuracy.

Accuracy is mainly concerned with both false positives along with false negatives of the intrusion detection mechanism, at the same time performance is measured by impact to the leading edge task response time distribution. Each of these metrics affects the end-user experience and critical factors determining even if the solution is practical for use in production systems. GUAN Xin, LI Yun-jie. (2011) explain, the intrusion prevention systems really have the ability of real-time defence and attack defence. IPS can attack an attacker can observe, In the near future, will be able to play in the field in the network security of its enormous power, Especially in national security Meharouech Sourour Bouhoula Adel Abbes Tarek (2009) They proposed a novel intrusion detection and prevention architecture where we combine the properties and characteristics wof the protected system in the process of traffic analysis. Guanlin Chen, Hui Yao, Zebing Wang. (2010) demonstrate Experimental results showed that this engine can not only detect and avert the main wireless attacks but also decrease false positives

REAL LIFE FAILURERS

Wireless Local Area Networks (WLANs), like many other networking technologies, needs to be secluded from the many security and intimidation issues. Even if some of the modern techniques have been intended to help ensure privacy for authenticated wireless LAN users, WLAN clients and venture infrastructure, your WLAN can still be susceptible to a diversity of threats that are unique to WLANs. Hackers may try to attack the system, or an employee may create a security violate that may leave the corporate WLAN or a client device vulnerable to attack.

Some particular security issues for WLANs are:

• Rogue APs: WLAN Access Points (APs) are economical, simple to install, and small in size such that a person can carry it. Unofficial WLAN APs can be associated with an enterprise network unwittingly or with malicious purpose, without the knowledge of IT—by easily carrying the device inside the enterprise and then connecting it to an Ethernet port on the network. Typically employees deploy rogue APs to get quick wireless access, they are mostly implemented with no WLAN security protocols (such as Access Control Lists, WPA, WPA2, AES, TKIP, 802. 1X, 802.11i, etc.). A virtual connection is possible to any Ethernet port on the networks, by cracking the present WLAN security control points. The building perimeter of an organization is not the restriction for area of coverage of rogue APs (unless you're using the paint), so bypassing these rogue APs it becomes possible for unjustified users to connect to the enterprise network. The prevention of such admission to the network is complicated as medium of wireless is invisible.

• MAC spoofing: APs in a WLAN transmit beacons (or probe responses) to broadcast their existence. The warning or guiding signals of an AP contain information about its identity i.e. MAC (media access control) address, and the identity of the network supported by it i.e. SSID (service set identifier). Wireless patrons listen to warning or guarding signals from different APs in the surrounding area. An AP that broadcasts the preferred SSID and transmits a strong warning or guarding signal, clients usually connect to such an AP.

• Honey pot APs: Multiple WLANs can co-exist in the one area, such that to any accessible network clients are allowed to connect, network can be either of their own network or another network in the surrounding area with overlapping network exposure. This allowance of admission to parallel WLANs can be exploited by hackers who set up an unauthorized wireless network by powering on an AP in the vicinity (e.g. street or parking lot) of your enterprise WLAN. "Honey pot" APs or "Evil Twins," are common for these APs, they entice authorized enterprise clients into connecting them by transmitting a stronger beacon signal and spoofing of MAC. An endorsed user unconsciously connecting to a honey pot AP creates security vulnerability by inadvertent provision of significant information of its identity like username, password. "Client mis-associations" i.e. Accidental connect of legitimate wireless clients in the organization WLAN to non-malicious neighbouring APs creating security weakness as the WLAN users may inadvertently provide confidential information to such APs and create a connection between your secure enterprise network and the neighbouring APs.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

• Denial of service: WLANs are being increasingly allocated with carrying mission-critical applications such as access to the database, Voice over IP, project data files, e-mail, and Internet access. These applications can be interrupted by a DoS (denial of service) attack, which causes downtime for network, user nuisance, and productivity thrashing. As it's a shared medium, transmissions of 802.11 Wireless LAN are effortlessly vulnerable to DoS attacks. Moreover, DoS attacks can be easily launched by exploiting "soft spots" in 802.11 MAC protocol. Most of the Wireless Networks are Highly Vulnerable to Hacking Attacks

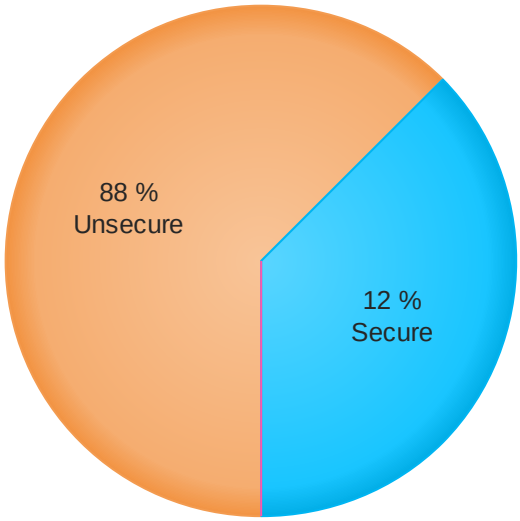

Fig. 1. Survey of Public Wi-Fi Networks

• Ad-hoc networks: The 802.11 WLAN standard has provisions for building peer to peer wireless connections between wireless users, so that further they can then shape up an ad-hoc network amid themselves. However, such networks (ad-hoc networks) can lead to security vulnerabilities.

The calmness of threats to enterprise network security from different types of APs like rogue, mis-configured, soft, also ad-hoc networks should not be ignored. Illegitimate devices linking to the enterprise network through such APs can take on data thievery, rerouting of data, and corruption of data, imitation, DOS (denial of service), virus insertion, and many more attacks. These vulnerabilities exist in both organizations that have official WLAN deployments and also those which have banned wireless usage.

PROPOSED SOLUTION FOR WIRELESS LAN SECURITY

Essential Security with WPA or WPA 2 Pre-Shared Key one more form of basic security now accessible is WPA or WPA2 Pre-Shared Key (PSK). The Pre Shared Key verifies users via a password, or identifying code both the client station and the AP (access point). A gain of access to the network for client can only be possible after password matching. This is implemented with the help of client's password and the password of an access point. An encryption key used for each packet of transmitted data is provided by TKIP or AES. For this encryption keying object is provided by the PSK. Though it is further secured than static WEP, PSK is alike to static WEP in that the PSK is stored on the client station and can be agreed if the client station is damaged or modified in a thievery. A well-built PSK security phrase which is a combination of alphabets, digits, and special (non-alphanumeric) characters is suggested. For very small businesses, or those that do not involve condemnatory data in their wireless LAN; Basic WLAN security that relies on a mixture of SSIDs, unlocked authentication, static (WEP) wired equivalent privacy keys, MAC validation, or WPA/WPA2 PSK is sufficient. Other corporations must endow in a security solution which is long-lasting and more powerful.

Better Security

Enhanced security is always recommended for those customers who require enterprise-class security. Advanced Encryption standard or temporal key integrity protocol through Cisco Unified Wireless Network provides complete hold for WPA and WPA2 with IEEE standard for communal verification and Temporal Key Integrity Protocol or Advanced Encryption Standard heading to WLANs that convey a superior wireless security solution. The Future computing Wireless Network includes the following:

- 802.1X for strong, mutual validation and run time for each user, for each session encryption keys
- TKIP for improvement to RC4 based encryption like key hashing (per-packet keying),
- AES for government-grade, highly secure data encryption Integration with the Self-Defending Network and NAC.
- Run time Intrusion Prevention System (IPS) efficiencies and advanced location services with real-time network accountability.
- Management Frame Protection (MFP) for burly cryptographic authentication of WLAN management frames

Remotely Access Wireless LAN Security

In certain instances, enterprises may require end to end security to protect their business implementations. With distant admission defence, controllers set up a virtual private network (VPN) which allows mobile users in unrestricted Wi-Fi at many civic places to channel back to the company network.

For enterprise deployments, an illustrated security solution, such as inline IPS for Wireless Network, satisfies and extends WLAN security requirements. Using VPN in an internal WLAN deployment may affect WLAN recital, limit roving and make the validation process more difficult for clients. Therefore, the extra efforts, restrictions, and expenditure of a VPN superimpose for an internal WLAN are unnecessary.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

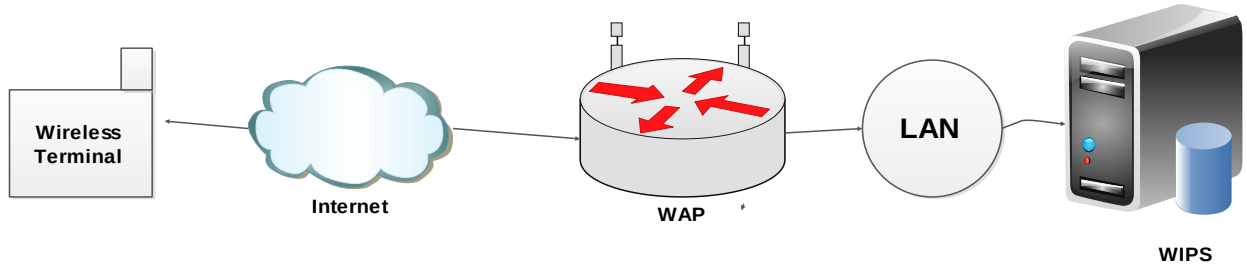

Fig. 2. WIPS frame work

CONCLUSION

We have proposed a system for the wireless prevention system for on an 802.11 wireless LAN. By using a MAC filtering mechanism, along with special network id to differentiate authorized and unauthorized client is able to differentiate between legitimate frames and forged frames. The scheme uses an inline strategy for validation of SSID. The proposed mechanism has low overheads and can be deployed in existing IEEE 802.11 WLANs. We have built and tested the prototype of the scheme. We have demonstrated that our mechanism can protect wireless clients against malicious management frame attacks launched at the layer 3. It focused on separation of legitimate TCP connection request with the SYN Flood attack packets. This and the other type of feature inline IPS techniques will be studied in future. Inline algorithms have been applied to a real IPS as its core classifier, deeply analysis of packet, soon afterwards.

ACKNOWLEDGMENT

We would to thank Dr **Navin kumar and Dr V M Thakare** for their valuable suggestions for the final write of this paper.

REFERENCES

[1] Yujia Zhang et al. An overview of wireless intrusion prevention systems, Volume: 1,pp 147-150,2010.
[2] S V Athawale; D N Chaudhari,Towards effective client-server based advent intrusion prevention system for WLAN,pp 1- 5,2015.
[3] Jiqiang Zhai, Yining Xie Researh on Network Intrusion Prevention System Based on Snort, August 22-24.pp. 1133 - 1136, 2011.
[4] N. Wattanapongsakorn, S. Srakaew, C. Charnsripinyo A Practical Network-based Intrusion Detection and Prevention System .pp 209 - 214, .2012.
[5] Fang-Yie Leu, and Zhi-Yang Li,.Detecting DoS and DDoS Attacks by using an Intrusion Detection and Remote Prevention System. Proceedings of the IEEE, pp. 251–254, .2009.
[6] Guanlin Chen; Hui Yao; Zebing Wang,Research of wireless intrusion prevention systems based on plan recognition and honeypot,pp 1-5, 2009.
[7] S.Vasanthi and Dr. S. Chandrasekar.a study on network intrusion detection and prevention system current status and challenging issues. IEEE IET, pp 181–183, 2011.
[8] Guanlin Chen, Hui Yao, Zebing Wang. Research of Wireless Intrusion Prevention Systems based on Plan Recognition and Honeypot.pp 1-5, 2009.
[9] Ricardo Koller, Raju Rangaswami,Joseph Marrero,Igor Hernandez, Geoffrey Smith. Anatomy of a Real-time Intrusion Prevention System.pp151-160, 2008.
[10] GUAN Xin, LI Yun-jie. An new Intrusion Prevention Attack System Model based on Immune Principle.pp 1-4, 2010.
[11] Meharouech Sourour, Bouhoula Adel, Abbes Tarek.Environmental Awareness Intrusion Detection and Prevention System toward reducing False Positives and False Negatives,pp 107-114, .2009.
[12] Xinyou Zhang ,Chengzhong Li ,Wenbin Zheng Intrusion Prevention System Design.pp 386-390, 2004.
[13] Guanlin Chen, Hui Yao, Zebing Wang. An Intelligent WLAN Intrusion Prevention System Based on Signature Detection and Plan Recognition, pp 168-172, 2010.

BIOGRAPHIES

Shashikant V. Athawale M Tech, CSE, currently teaches graduate and postgraduate level Student in Computer Science and Engineering at Pune University in Pune Maharashtra, India. He is currently a Ph.D.candidate in computer science at the Amaravati University in Maharashtra, India. He has worked extensively in both the wired and wireless network sectors to improve the network security of their critical information systems. His research focuses on Intrusion detection and prevention system developing the security of computer and wireless & Ad hoc network systems.

Dr. Mahendra A Pund is working as Professor in Computer Engineering Department at Prof. Ram Meghe Institute of Technology & Research, Badnera-Amravati, India. He has 22 years experience in teaching profession. Total 24 papers are published in International &National Conferences and International Journals. His research interest is in the areas of wireless network, ad hoc network and security issues, Image processing, Machine Learning, Image Processing and Pattern Recognition, Feature Extraction. He is guiding many research scholars and he is a member of CSTA, New York, CSI, ISTE, Associate Member of I.E, IACSIT, Singapore and IAENG, Hong Kong. Also, he is Advisory consultant to Cape Arc Solutions Pvt. Ltd. (www.capearcsolutions.com), Consultant to New Gen Systems pvt.ltd.