Aims and scopes: The journal publishes refereed, high quality original research papers in all areas of engineering sciences and related applied sciences.

Call for papers: Authors are cordially invited to submit papers to the editorial office by e-mail to: ces@mhikari.com. Manuscripts submitted to this journal will be considered for publication with the understanding that the same work has not been published and is not under consideration for publication elsewhere.

Instruction for authors: The manuscript should be prepared using LaTeX or Word processing system, basic font Roman 12pt size. The papers should be in English and typed in frames 14 x 21.6 cm (margins 3.5 cm on left and right and 4 cm on top and bottom) on A4-format white paper or American format paper. On the first page leave 7 cm space on the top for the journal's headings. The papers must have abstract and keywords. The references should be in alphabetic order and must be organized as follows:


Editorial office
e-mail: ces@mhikari.com

Postal address: HIKARI Ltd, P.O. Box 85 Ruse 7000, Bulgaria
Street address: HIKARI Ltd, Vidin str. 40, office no. 3 Ruse 7012, Bulgaria

www.m-hikari.com
Published by Hikari Ltd
Contents

Misug Gu, Jeonghee Hwang, Taeil Kwon, Keunho Ryu,  Implementation of semantic information retrieval system in mobile environment  603

Sunghyu Han, Hee Suk Seo, Seunghwan Ju,  Efficient calculation of the weight distributions for linear codes over large finite fields  609

Jae Jung Kim, Seng Phil Hong,  Study on the privacy-preserving vehicular PKI in autonomous driving environments  619

Kyoungsik Min, Seung-Woan Chai,  A comparative analysis of personal data protection policies of leading countries in the internet of things (IoT) environment  627

Kyungyoung Ohk, Seunghae Park, Kyoung Sik Min,  The effect of personal information security attitude and perceived company information security policy on mobile banking acceptance  635

Chang-Su Kim, Chu Xun, Hoe-Kyung Jung,  A study on the Kismet-based wireless intrusion prevention system  641

Seung Min Ryu, Si Young Lee, Chang Woo Ryu, Seong Gon Choi,  A method of the first-N packets storage by using the advanced-PCA  647

Soon Ki Eun, Jeong Sik Kim, Seong Gon Choi,  Implementation of power management system by using data clustering method  655

Hyeon Yang, Jeong Sik Kim, Seong Gon Choi,  Power consumption control method using pattern analysis for load distribution  663

Evgeny Nikulchev, Dmitry Ilin, Dmitry Biryukov, Gregory Bubnov,  Monitoring of information space for professional skills demand  671
Dedi Irawan, Rado Yendra, Hartono, Okfalisa, *Normalized power propagation on 1x6 fiber coupler* 679

Jaegwi Go, Je-Hyun Lee, Seokmin Joo, *Elastic characteristics of a non-symmetric laminated composite roller guided panel through mathematical approach* 689

Nazgul Kaliyeva, Zaure Rakisheva, *Stabilization of the small spacecraft with electromagnetic actuator in the presence of a residual magnetic moment* 705

Yasushi Itoh, Hiroaki Takagi, *L-Band SiGe HBT dual-band differential amplifiers having frequency-tunable bandpass or bandstop responses using novel varactor-loaded dual-band resonators* 713

Yasushi Itoh, Hiroaki Takagi, *L-band SiGe HBT active differential equalizers with varactor-tuned bias circuits for variable, positive or negative gain slopes* 727

Dharma Arung Laby, Sungkono, Bagus J. Santosa, Ayi S. Bahri, *RR-PSO: fast and robust algorithm to invert Rayleigh waves dispersion* 735

Idanis Diaz Bolano, German Sanchez Torres, *A clustering-based method for brain tumor segmentation* 743

Leonid Gurevich, Dmitry Pronichev, Mikhail Trunov, *The stress-strain state of Ti/Al composites with elliptical defects and soft interlayers under tensile loading* 755

Nuramirah Akrom, Zuhaimy Ismail, *EMD-DR models for forecasting electricity load demand* 763

Konstantin Moiseевич Zingerman, Dmitry Alekseevich Shavyrin, *An approximate analytical method for stress analysis in a viscoelastic body with a circular inclusion considering the geometric and physical nonlinearity* 781

Umi Mahdiyah, Elly Matul Imah, M. Isa Irawan, *Integrating data selection and extreme learning machine to predict protein-ligand binding site* 791
A Study on the Kismet-Based Wireless Intrusion Prevention System

Chang-Su Kim, Chu Xun and Hoe-Kyung Jung*

Department of Computer Engineering, Pai Chai University, Daejeon, Korea
*Corresponding author

Abstract

Recently, the use of wireless networks that can be used conveniently increases due to the increasing number of people who are using internet and smart devices. Comparing with the wired network, the wireless network can be operated cheaper but it has weakness in security problems.

In this paper, we propose a system to detect and prevent security threats that occur in a wireless environment. The system detects security threats using the open source-based, Kismet and Wireshark and uses Iptable to prevent intrusion. We use a hacking tool that is used for the simulation in order to verify the compliance.

Keywords: Wireless Environment, Security, Iptable, Kismet, Wireshark

1 Introduction

Because of the advances in wireless communication technology and increasing use of smart devices, a number of users who use wireless network increases. Since the wireless network uses radio waves to send and receive data, it meets the network conditions required by the portable devices. In addition, the use of wireless network keeps increasing because of the convenient availability compared to wire network. However, wireless network has disadvantage in security compared to wire network. And wireless network users may use wireless network indiscriminately lacking both the security knowledge and the importance of security. Due to these problems, wireless network users can be exposed to the misuse crime [1, 2, 3].
In this paper, we suggest a system which can detect and then block security threats in wireless network environment by using kismet, wireshark and Iptable. In order to validate the performance of the suggested system, we reproduce attack conditions in a wireless network by employing tools used in hacking. And, by using kismet, we collect packets of hacking tools and analyze collected packets with wireshark. The analysed packets are applied to the Iptable rules and prevent system invasion by blocking corresponding packets and IP.

2 Related research

2.1 Vulnerabilities of wireless network security technologies
IEEE 802.1x is a standard technology that is being used in an Ethernet network environment, to authenticate the client. By referring the registered user information in RADIUS, server shall judge whether to allow network access by checking that the accessing AP user is registered in RADIUS server. And, in exchange of authentication message, EAP (Extensible Authentication Protocol) is used and data is being encrypted by using the WEP. The security vulnerability of IEEE 802.1x is the weakness of brute force and MITM (man in the middle attack). These causes are due to the vulnerable issues with EAP and WEP [4, 5].

2.2 Wireshark
Wireshark is a program developed to manage the network. Using wireshark enables to save network packets and to analyze the saved packets in detail. Wireshark can use the data in other packet programs and support a wide variety of operating systems with UNIX or Linux, widows, etc. And it also provides the ability to search for specific packet, which further enables one to effectively analyze the packets [6].

2.3 Iptable
Iptable is a processing system for network packet in Linux kernels, and it was developed from netfilter project. Iptable filters TCP and UDP, controls a specific port, and thus prevents intrusions by a malicious user. Iptable consists of table and chains, requiring root permission. Tables perform features such as packet filtering or network address translation and consist of the four tables like Filter, NAT, Magle, and Raw.

3 Wireless intrusion prevention system design and construction

3.1 Wireless intrusion prevention system design
In a wireless network environment, one can't detect security threats raised from system used in a wire firewall. To operate reliably on wireless network, one needs a wireless intrusion prevention system with a continuous monitoring function and integrated management. In this paper, suggested system configuration is shown in Fig. 1.
By using Kismet, one collects packets in a wireless network, inspects AP, and detects trespass. The collected packets use Wireshark to analyze pattern of attack. And, based on the analysed patterns, Iptable’s rules are created to prevent intrusion.

3.2 Wireless intrusion prevention system construction

Suggested wireless intrusion prevention system consists of a server and a client. The server of wireless intrusion prevention system consists of kismet and wireshark, Iptable to block intrusion. The client of wireless intrusion prevention systems consists of kismet, wireshark and hacking tools, which are used to inspect mock hacking and wireless network environment. The server construction order to build a wireless intrusion prevention system is as follows.

(1) Installation of linux operating system of CentOS 6.4
(2) Installation of Rpmforge package required for installing kismet
(3) Kismet installation and environment configuration
(4) Wireshark installation and environment configuration
(5) Iptable Installation

4 Experiments

4.1 Experimental environment

In this experimental environment, one uses PC used as a server in wireless intrusion prevention system and two laptops used as client. And, the experiment was conducted using one wired router and three wireless routers. The configuration of experimental environment is shown in Fig. 2.
4.2 Experimental method

The experiment proceeds with WPA shared key crack, and MITM attack. A Details for each attack is as follows.

(1) WPA shared key crack
   • Use Airmon-ng, Generate the monitor interface
   • Use Airodump-ng, Gather information of the surrounding AP
   • Use Airodump-ng, Collect information from target AP
   • Use Aireplay-ng, Launch with replay attack
   • Use Airodump-ng, Collect WPA handshake
   • Use Aircrack-ng, Launch with dictionary attack

(2) MITM attack
   • Use Airmon-ng, Generate the monitor interface
   • Use Airbase-ng, Generate AP
   • Generate a bridge consisting of wired and wireless

4.3 Experimental results

1) WPA shared key crack
   Blocking the packets used in replay attack and complicating the password lead to a failure of dictionary attack. Replay attack is shown in Fig. 3, which is a screen analyzing the used packets with Wireshark.
A study on the Kismet-based wireless intrusion prevention system

2) MITM attack

AP used in MITM attack can detect the same way as honeypot AP attack is detected. In addition, using the packet information can detect MITM attack. Packets of MITM attack analyzed with Wireshark are applied with the rule of Iptable as shown in Fig. 4.

![Fig. 4. Prevention of man-in-the-middle attacks with Iptable](image)

5 Conclusion

In this paper, we suggested the system to prevent the security threats by detecting and blocking security threats on a wireless network. The server of wireless intrusion prevention system implements the system by using the kismet and wireshark, Iptable. And, client of wireless intrusion prevention system consists of kismet and wireshark, and hacking tools.

Wireless intrusion prevention systems collects the packets of wireless network as Drone of Kismet, and then Kismet saves the collected packets in files. And, the system uses kismet to inspect wireless network environment and detect illegally cloned AP or unauthorized AP. Wireshark is used to analyze the packet files, saved
as kismet while those packets analyzed with Wireshark are transformed to the rules of Iptable. Once Iptable rules are generated, the system makes sure that invasion is blocked, and if the block is unsuccessful, Iptable rules are re-generated.

In this paper, in order to verify suitability of the suggested wireless intrusion prevention system, the system progresses mock hacking using hacking tools of client, analyzes the packets of mock hacking using wireless intrusion prevention system, and prevents trespass by adding rules. By using wireless intrusion prevention system suggested in this paper, one can expect an improved wireless network security in operating facilities using UNIX or Linux based server. Also, the system can be effectively used to users who intend to learn wireless network security.

For the future research, it is necessary to combine the suggested wireless intrusion prevention system and Snort in order to even detect a wired network.

References


http://dx.doi.org/10.6109/jicce.2014.12.3.154

http://dx.doi.org/10.4028/www.scientific.net/amr.1049-1050.1993


Received: May 19, 2015; Published: June 2, 2016