International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 10, Issue 7 (July 2014), PP.81-84

Tracking rogue device in wireless Network System

[1]Prof. Amolkumar N. Jadhav, [2]Prof. Shounak Sugave,
[3]Prof. Hanmant Magar, [4]Prof. Chudaman Sukte
[1,2,3,4]Assistant Professor MIT College of Engineering, Pune India

Abstract:- Rough Device is one of the leading security threats in current network scenario, if not properly handled in time could lead from minor network faults to serious network failure. Most of the current solutions to detect rough device are not automated and are dependent on a specific wireless technology. In this p deviceer I used the integrated solution for detection and eliminate the rogue Device. Rogue detection algorithm is also proposed. This Methodology uses two properties: (1) doesn't require any specialized hardware; (2) the used algorithm detects and completely eliminate Rough device from network; this solution is effective and low cost.

Keywords:- Rogue device , Wireless Security, Mobile Agents,Wireless LANs.

I. INTRODUCTION

Many organizations utilize the wireless LAN to provide the access channel to the Internet and Intranet enabling the flexible workforce. Employees are able to move their computers from one location to another. While doing so, communications with peers and the Internet are continuously maintained. It has been clearly shown that utilizing wireless LAN helps increasing the productivity of a company that is using it. However the wireless security is always a primary concern. The information transmitted by the users is broadcasted through the air. Everybody within range of the wireless signal can easily tune in and device ture the data. Most enterprise wireless implementations normally include the wireless security measure such as IEEE 802.11i or WPA (Wireless Protected Access). IEEE 802.11i provides the encryption and authentication mechanisms to protect user from unauthorized access and data eavesdrop over the wireless network. However, such security measures cannot protect the system from the unauthorized installation of the device by their own staffs. The staffs can easily plug in the unauthorized device (normally called rogue device) to the network for their personal usage. Most staffs are unaware of the security threats that come along with this act. The unauthorized user or hacker can bypass the company's line of network defenses (i.e., firewall, access control) through the rogue device and poses the serious threat to the organization.

A Rogue device is typically referred to as an unauthorized DEVICE in the literature. It is a wireless device that has either been installed on a secure network without explicit authorization from a local administrator, or has been created to allow a cracker to conduct a man-in –the middle attack or can be used by adversaries for committing espionage and launching attacks.

Rogue devices are present on about 20% of all enterprise networks. Often these "Rogue" devices might be installed by valid user attempting to increase the range of the network but doing so without proper authorization. This usually results in a security hole that may be exploited by intruders, or intruder himself planting an DEVICE with a higher broadcast power than normal to masquerade as a legitimate device

1) Access Point 2) Switch 3) Central System

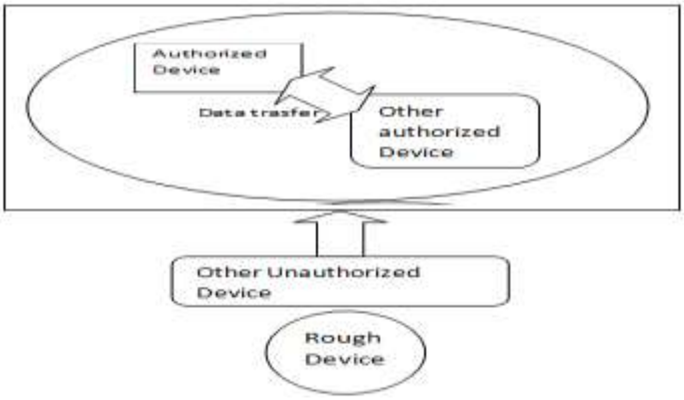


Fig. Rough device is trying to access data share between them with high signal.

Approach For Detecting Rough Devices :

This algorithm is proposed by Prof S. B. vanjale Most of the current deviceproaches for detecting rogue DEVICEs are rudimentary and easily evaded by hackers. Some organizations have equipped IT personnel with wireless packet analyzer algorithm fig-1, forcing IT personnel to walk the halls of the enterprise or campus searching for rogue DEVICEs. This method is generally ineffective because manual scans are time-consuming and expensive – and, therefore, are conducted infrequently. Also, with 802.11 hardware operating at separate frequencies (802.11a - 5Ghz and 802.11b - 2.4Ghz), IT personnel must upgrade their detection devices to accommodate multiple frequencies. Moreover, scans are easy to elude, since a rogue DEVICE can easily be unplugged when the scan takes place.[1]

Wireless Traffic Analyzer Algorithm:-

```
For (each flow between sender and receiver)
{ n =0
for (the first N packet)
{ n = n+1;
$\Delta Tn = Tn + Tn+1$
// Tn is arrival of n th packet
Comput the median of inter arrival times $M(\Delta Tn)$
If ( $M(\Delta Tn) \leq 5ms$ )
Then classify sender as ethernate
Else
Specify the sender as a wireless }
```

The potential rogue device data is stored in the database waiting for analyzed. Central system analyzes the rogue devices based on the detection algorithm shown in Figure 2. The algorithms are the follows:

1) Compare the sniffing data (i.e., SSID, Wireless MAC) with the authorized DEVICE information. The authorized DEVICE information is stored beforehand. There are three possible outcomes: Completely Matched (SSID and MAC), Completely Unmatched (not SSID and not MAC) and Partially Matched (not SSID but MAC, or SSID but not MAC). If completely matched, goto stage 2). If Partially Matched, goto stage 3) and If Completely Unmatched goto stage 4)

2) For Completely Matched, there are two possibilities of devices: Trusted DEVICE or Attacker Rogue device. The attacker rogue device completely spoofs the authorized device information (i.e., spoof MAC and spoof SSID). Typically it is hard to verify if an device is the legitimate one. Therefore, we propose the technique that can differentiate Trust devices from Spoof Rogue DEVICE using timestamp information within Beacon. Normally each Device will includes the timestamp on the Beacon. The timestamp is total uptime of the device measured since its start. Even though the attackers can manipulate the spoof SSID and wireless MAC, they will have the difficult time trying to synchronize and spoof timestamp of the trusted device.

3) For Partially Matched, the result would be either Misconfiguration DEVICE or Attacker's Rogue DEVICE. The Misconfiguration DEVICE is the device with configuration that is not consistent to the registered DEVICE. Verifying the configuration of all DEVICEs will remove the outcome of Misconfiguration DEVICE and leave remaining of Attacker's Rogue DEVICE.

4) For Completely Unmatched, the result would be either Neighborhood DEVICE or Employee rogue DEVICE. If the DEVICE connects to the external network, we can assume that it is Neighborhood DEVICE. If the DEVICE connects to the internal network, it is Employee rogue DEVICE. The technique to perform "DEVICE internal connection checking" or DEVICE localization is described in the next section.

The potential rogue device data is stored in the database waiting for analyzed. Central system analyzes the rogue device based on the detection algorithm shown in Figure 2. The algorithms are the follows:

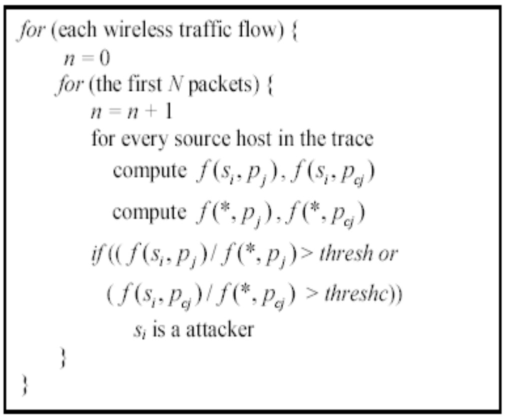
1) Compare the sniffing data (i.e., SSID, Wireless MAC) with the authorized DEVICE information. The authorized DEVICE information is stored beforehand. There are three possible outcomes: Completely Matched (SSID and MAC), Completely Unmatched (not SSID and not MAC) and Partially Matched (not SSID but MAC, or SSID but not MAC). If Completely Matched, goto stage 2). If Partially Matched, goto stage 3) and If Completely Unmatched goto stage 4)

2) For Completely Matched, there are two possibilities of devices: Trusted DEVICE or Attacker Rogue DEVICE. The attacker rogue DEVICE completely spoofs the authorized DEVICE information (i.e., spoof MAC and spoof SSID). Typically it is hard to verify if an DEVICE is the legitimate one. Therefore, we propose the technique that can differentiate Trust DEVICEs from Spoof Rogue DEVICE using timestamp information within Beacon. Normally each device will include the timestamp on the Beacon. The timestamp is total uptime of the device measured since its start. Even though the attackers can manipulate the spoof SSID and

wireless MAC, they will have the difficult time trying to synchronize and spoof timestamp of the trusted DEVICE.

3) For partially matched, the result would be either Misconfiguration DEVICE or Attacker's Rogue DEVICE. The Misconfiguration DEVICE is the device with configuration that is not consistent to the registered DEVICE. Verifying the configuration of all DEVICEs will remove the outcome of Misconfiguration DEVICE and leave remaining of Attacker's Rogue DEVICE.

4) For Completely Unmatched, the result would be either Neighborhood DEVICE or Employee rogue DEVICE. If the DEVICE connects to the external network, we can assume that it is Neighborhood DEVICE. If the DEVICE connects to the internal network, it is Employee rogue DEVICE. The technique to perform "DEVICE internal connection checking" or DEVICE localization is described in the next section.



```
for (each wireless traffic flow) {
    $n = 0$
    for (the first $N$ packets) {
        $n = n + 1$
        for every source host in the trace
            compute $f(s_i, p_j), f(s_i, p_{cj})$
            compute $f(*, p_j), f(*, p_{cj})$
        if(( $f(s_i, p_j) / f(*, p_j) > thresh$ or
          ( $f(s_i, p_{cj}) / f(*, p_{cj}) > threshc$))
            $s_i$ is a attacker
    }
}
```

In this section, we perform the experiment to show how the proposed system can detect the various types of rogue access point. We define four types rogue device.

1.Rogue Type 1: Employee's rogue access point, no SSID spoof and no wireless MAC spoof
2.Rogue Type 2: Attacker's rogue access point, with SSID spoof but no wireless MAC spoof
3.Rogue Type 3: Attacker's rogue access point, with no SSID spoof but wireless MAC spoof
4.Rogue Type 4: Attacker's rogue access point, with Rogue SSID spoof and wireless MAC spoof.

II. CONCLUSION

In this paper I propose the Detecting & Eliminating the rogue device. Classification of rogue Device and related risk assessment is analyzed. Rogue detection algorithm is also proposed. Our proposed solution is effective and low cost. It is designed to utilize the existing wireless LAN infrastructure. There is no need to acquire the new RF devices or dedicated wireless detection sensors. The experiments in the real system are demonstrated.

REFERENCES

[1]. Detecting & Eliminating Rogue device in IEEE 802.11 WLAN S.B.Vanjale, Amol K. Kadam, Pramod A. Jadhav Department of Computer Engg. Bharati Vidy deviceeeth Deemed University College of Engineering Pune svanjale@rediffmail.com, akkadam@bvucoep.edu.in, pramodjadhav1408@gmail.com

[2]. Detecting and Eliminating Rogue Access Points in IEEE-802.11 WLAN - A Multi-Agent Sourcing Methodology V. S. Shankar Sriram1, G.Sahoo3 Department of Information Technology, Birla Institute of Technology, Mesra, Ranchi, India sriram@bitmesra.ac.in, drgsahoo@yahoo.com

[3]. Cisco Wireless LAN Controller Configuration Guide, Release 5.0—http://www.cisco.com/en/US/products/ps6366/products_configuration_guide_book09186a008082d572.html.

[4]. NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems, provides details on access control issues, and developing and updating security plans.

[5]. NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, gives information on coordinating contingency planning activities.

[6]. John Bellardo and Stefan Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions", 2003, Usenix 2003 Proceedings. http://www.cs.ucsd.edu/users/savage/papers/UsenixSec03.pdf Retrieved Jan 20, 2004.

[7]. IEEE, *IEEE 802.11 standards documents*, http://standards.ieee.org/wireless/ . Retrieved Jan 20, 2004

[8]. Tom Karygiannis and Les Owens, Wireless Network Security: 802.11, Bluetooth and Handheld Devices, National Institute of Standards and Technology Special Publication 800-48, November 2002.

http://cs-www.ncsl.nist.gov/publications/ nistpubs/800-48/NIST_SP_800-48.pdf . Retrieved Jan 20, 2004

[9]. Rob Flickenger, *Wireless Hacks: 100 Industrial-Strength Tips & Tools, 286 pages*, O'Reilly & Associates, September 2003, ISBN: 0-596-00559-8

[10]. Joshua Wright, “Detecting Wireless LAN MAC Address Spoofing”, Retrieved on Jan 20, 2004. http://home.jwu.edu/jwright/

[11]. Suman Jana and Sneha Kumar Kasera. On fast andaccurate detection of authorized wireless accesspoints using clock skews. In MobiCom ’08:Proceedings of the 14th ACM international conferenceon Mobile computing and networking, pages 104–115.ACM, 2008.

[12]. Lanier Watkins, RaheemBeyah, Cherita Corbett “A Passive Approach to Rogue Access Point Detection” 1930-529X/07/$25.00 © 2007 IEEE

[13]. Potential Security Threats of a wireless network http://www.infosecwriters.com/text_resources/pdf/Wireless_JMeyer.pdf

[14]. Threats to Wireless Local Area Network (WLAN) and Countermeasures” ,A.V.Dhaygude, K.R. Patil, A.A.Sawant ,ICONS’07,January 27-29,2007,Ero de,Tamilnadu,India.

[15]. Suman Jana and Sneha Kumar Kasera. On fast andaccurate detection of nauthorized wireless accesspoints using clock skews. In MobiCom ’08:Proceedings of the 14th ACM international conferenceon Mobile computing and networking, pages 104–115.ACM, 2008