International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 11, November - 2013

Security Breach: Denial of Service Attack

Sumesh Kadam
Vishwakarma Institute of Information Technology, University of Pune

Abstract

Modern world of network security has recently become a thriving and fast-moving discipline. As network systems are becoming lifeline of electronic mass and communication there is urge to provide the security to these network system. People belonging to divergent interests, incentives are using networks to fulfill their purpose. To protect the network from the malicious user's the concept of the network security emerges. This document provides valuable insights not just into 'security' topics such as privacy, bugs, spam, and phishing, but into more general areas such as system dependability and configuration

Index Terms-DOS, 802.11, MAC

1. Introduction

Network security is a level of guarantee that all the machines in a network are working optimally and the users of these machines only possess the rights that are granted to them. This include preventing unauthorized people from acting on system maliciously preventing users from performing involuntary operations that are capable of harming the system securing data by anticipating failures guaranteeing that services are not interrupted.

2. The Causes of Insecurity

Insecurities are generally broken down into two categories .An active state of insecurity due to user ignorance of the system's functionalities, some of which can be harmful to the system [1]. A passive state of insecurity when the administrator a system is not familiar with the security mechanisms that are in place.

Attackers have divergent motives i.e. - The appeal of forbidden to make analysis if network security can be broken. A desire for money Attacker harming the network intentionally. The goal of attackers is often to take control of a machine in order to be able to perform desired actions. There are different ways for obtaining information that can be used in attacks by exploiting system weaknesses by using force to crack a system.

3. Exploiting the Network

Denial of Service attack are implemented by either forcing the targeted computer to reset or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately. The strong point of this type of attack-Network connectivity attack launched with a little effort is difficult to trace attack back to its originator. Any Access Point are susceptible that are using 802.11 Protocol.

4. Physical Layer Vulnerabilities

IEEE 802.11 uses 2.4 GHz frequency band and 2-11 GHz bands at physical layers. DoS attack can be launched against physical layer by using radio jamming device or a source of strong noise to interfere the physical channels and may compromise the service availability. However this kind of attack is not common as it need specialized hardware equipment to be launched, furthermore jamming attacks can be detected using radio analyzers. It can create great problems during exchange of sensitive information or during warfare. For jamming attack in IEEE 802.11, the attacker needs to be close to the target Access Point. The attacker can launch the attack from anywhere. Due to the vast coverage area and dense deployment of wireless mesh routers it is more vulnerable to physical layer DoS attacks. Currently IEEE 802.11 uses Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS). The mechanism is capable enough to handle the jamming attack on these broadband wireless networks

5. Link Layer Vulnerabilities

The IEEE 802.11 MAC uses shared medium amongst the nodes and is highly vulnerable to attack and collisions. The current mechanism of CSMA/CA with RTS/CTS can be compromised for MAC layer DoS attack either by sending bulk of MAC control messages to an innocent neighbor or by holding the MAC channel for unnecessary continuous transmission keeping a legimate node back. .

6. Implementation

Successful trials have been tried out. Different access point with different security mechanism have been tested.

The attacker side consists of four functional units:

- User interface
- Packets
- Wireless Adapter
- Wireless communication layer

The target side consists of three functional units:

- Wireless Adapter
- Wireless communication layer

Algorithm-
User interface at Attacker's End

```
Start
1.   Search Channel that is broadcasting.
2.   If channel not present then
             Search Channel
     Else
             Show channel present
             Display Channel Details
             Select Attack
             Initiate the Attack
             Display Information
             If input=close then
             Stop attack
     End
```

8. Results of DoS Attacks

The results of different DoS attacks on broadband wireless networks vary with the nature and type of DoS attack.

- ➢ Decrease timeout period
- ➢ Reset the connections sooner
- ➢ Can deny legitimate access where the timeout period will be less than the round trip times
- ➢ Increase the number of half-open connections
- ➢ More connections at the same time
- ➢ Will increase the use of resources

9. Countermeasures

DoS attack is of low intensity, if launched against a single node either to exhaust its battery or to isolate it from the network operations [2].

• DoS attack is of high intensity if it is launched to make services unavailable for a target area in wireless broadband networks.

• Dos attack will be of highest intensity if it is launched to cripple down the entire broadband wireless network by distributive flooding. Distributed flooding is normally used for this purpose to exhaust the bandwidth of the network or to overflow the resources of the gateways. DoS in any form against any network are regarded as a severe attack. Some possible countermeasure needs to be investigated to overcome to some extent against DoS and related issues in broadband networks.

• Current encryption mechanisms used in these broadband networks are WEP, DES, and AES, which are vulnerable to eavesdropping kind of attack. Improved and efficient encryption mechanisms needs to be proposed exclusively for each of the broadband technology, as successful eavesdropping later on facilitate the attackers to launch DoS attacks[3].

• A location detection mechanism based on the signal strength needs to be devised for the AP and wireless mesh router with the ability to identify a malicious node for flooding probe request and de-authentication kinds of attacks [4].

• Improved routing protocols are desirable particularly for the multi-hop.

10. Conclusion

Even though the increasing knowledge and understanding of the computer systems. Most of the home user are not aware how to handle the Network Security. This lack of understanding leaves many home systems open to attack.

References

[1] D.R. Raymond and S.F. Midkiff, “Denial of service in wireless sensor networks: attacks and defences,” IEEE Security and Privacy, Vol.7, No.1, pp. 74-81, March 2008.

[2] "How To: Harden the TCP/IP Stack Against Denial of Service Attacks in Windows 2000" Article ID: 315669 - Last Review: March 27, 2008.

[3] Camp J. and Knightly E., The IEEE 802.11s extended service set mesh networking standard, *IEEE Communication Magazine*, **46(8)**, 120-6 **(2008)**

[4] Steve Glass, Marius Portmann and Vallipuram, securing wireless mesh networks, IEEE computer society-1098-7801-2008@IEEE0