Secure Routing in IoT Networks

Hassan Sreedhar, Nisarga (MS Electrical Engineering)
Sudheera Kalyankar, Sanjana (MS Electrical Engineering)

Introduction

- MIM attack is a type of attack where an intruder captures data going between two devices.
- Using Kali Linux, attack is performed on a client to access the login credentials.
- This attack is then detected utilizing Wireshark software.
- Also, tools such as Driftnet are used to capture images viewed by the victim machine.
- URL Snarf is one tool used to grab a list of all the URLs visited by the victim machine.

Methodology

Model 1
- This model shows the Man in the Middle attack using the old-fashioned Manual Method.
  - ARP spoofing
    - It is carried out by using the tool "arp spoof" preinstalled in Kali Linux.
    - Attacker spoofs the victim machine and captures the login credentials while logging into a test website.
  - This can be viewed on the terminal of the Kali Linux machine.

Driftnet
- Tool used to capture images viewed on the victim machine.

Model 2
- This model performs the same actions as model 1 but uses a preinstalled Kali Linux tool called Ettercap.
  - Unified spoofing is performed in Ettercap for this project.
  - Here the victim and gateway router are added as the target 1 & 2.

Detection
- Attack can be detected by using the command "arp --a" on the command prompt of the victim machine.
- It can be noticed that, two IP addresses have the same MAC address.
- That is the router’s MAC address is duplicated by the attacker machine to display itself as the router.

Detection using Wireshark
- The login credentials are captured using Wireshark which can be viewed by opening a HTTP packet.
  - A HTTP GET message contains the username and password that has been spoofed from the victim machine.
  - The same test website is used to login and that is captured.

Comparing attacks of two models
- Time consumption is lesser in model 2 compared to model 1.
- Port forwarding must be carried out initially to perform spoofing in model 1. But model 2 starts off directly using Ettercap.

Comparing detection of two models
- In model 1, detection is performed by providing a command on the command prompt.
- Here, it was carried out using wireshark which was clearly visible with the yellow color duplication indication.
- It is important to note that, the time consumption was lesser in model 1 than in model 2 during detection.

Summary/Conclusions

- Some of the best practices to avoid MIM attacks are:
  - By providing a strong mechanism of encrypting the wireless access points to prevent unauthorized users from entering the network.
  - By using a Virtual Private Network to create a secure environment.
  - One of the major and most important prevention techniques is by the use of HTTPS to securely communicate over HTTP.

Key References