A Monitor System to Detect Botnet Activity in IoT Based Home Automation System

Shrisha H S

Assistant Professor
Department of Computer Science & Engineering
Canara Engineering College
Mangaluru, Karnataka, India

Anupama V

Assistant Professor
Department of Computer Science & Engineering
Canara Engineering College
Mangaluru, Karnataka, India

***Abstract*— Emerging Internet of Things (IoT) technology has given new tools and means for developing Home Automation Systems to create smart homes [1]. Functions which are handled smartly are climate control, home electronics, security systems, lighting and much more to come. Malwares can cause abnormal behaviour in the connected smart devices. So to monitor, detect and take corrective measures, a monitoring system is proposed.**

***Keywords*—Internet of Things (IoT), Home Automation Systems, Safe State**

I. INTRODUCTION

In an IoT based Home automation System there may be a *Manager Application* [1] which recognizes the devices and activates them. A web server may have manger application which translates browser instructions to action or a *Centralized Intelligent Home Controller* [2] or a simple mobile app at low cost products.

The motivation behind Home Automation is Comfort, Energy conservation, Efficiency in usage of smart appliances[2]. All these motives are need of the day and more smart home appliances connect to internet. These smart devices may be vulnerable to attacks. Malware are getting sophisticated day by day and it is easy to attack Home Automation System because most of the customers are not technology aware.

If a malware intrudes to a Home Automation System, it can steal device usage information, take control of devices, and harm the devices which can cause damage to house, people and also reputation of the vendors. This paper proposes a monitoring system in detecting malware activities in Home Automation Systems.

Malware can be a Trojan, Spyware, Virus, Worm, and Backdoors. Trojans mainly aim at taking over devices under intruder control to perform, for example Denial of Service attack, Spyware may send information about the devices to intruders, Backdoors can allow intruders to connect to home automation networks, and Virus and worms can damage the software.

II. HOME AUTOMATION SYSTEM MONITOR

House Automation System monitor consists of a Master and slave monitors. Master monitor is installed in *Manager Application* or in general words central controlling software of the Home Automation System. Slave monitors are installed in smart devices. Slave monitors give regular reports about the behavior of connected smart devices. Reports consist of data including but not restricted to bandwidth usage of devices, recognizable software list installed in the devices, memory usage. If there is any anomaly in the behavior of the smart devices then the monitor will notify the user by highlighting the particulars.

III. SAFE STATE

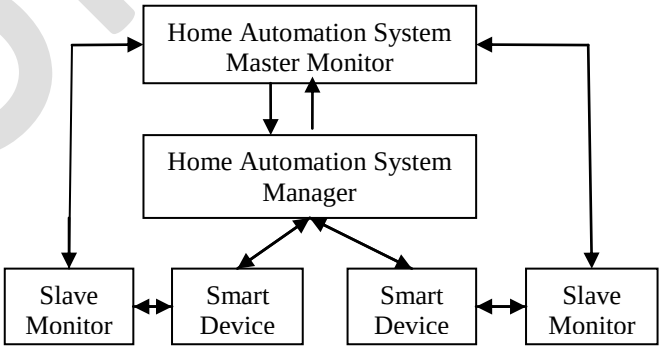

Figure 1: Monitor system architecture

When the system is installed by the vendor in user homes the Home Automation System Monitor, the Monitor records the devices installed, its software, bandwidth usage , access patterns and consider itself in *Safe State*. If there is an update of installed software it should be authenticated by the vendor and inform the Monitor that devices are in *Safe State*. Once the Monitor considers itself in *Safe State*, the device activity at the time of vendor marking the system as *Safe State* is taken as benchmark. Slave monitor while generating device activity reports will compare current device behavior with *Safe State* benchmark and based on comparison anomalies is reported. Slave Monitors maintain a time stamp table named *Safe State*

time stamp to keep track of time when the system was marked to be in *Safe State.*

IV. SLAVE MONITORS OPERATIONS

Slave Monitor performs DISABLE, SANITIZE, and MASTER RESET, SELECTIVE SANITIZE operations on Smart Devices.

- DISABLE is a command issued by Master Monitor to Slave Monitor. Upon receiving DISABLE command Slave Monitor deactivates or switch off the selected smart device.
- SANITIZE is a command issued by Master Monitor to Slave Monitor. Upon receiving SANITIZE command Slave Monitor resets the device to previous accepted *Safe State* and remove all the software updates which was installed after recent *Safe State time stamp.*
- MASTER RESET is a command issued by Master Monitor to Slave Monitor. Upon receiving MASTER RESET command slave monitors reset the smart device into factory configuration removing all the updates including *safe state time stamps*.
- SELECTIVE SANITIZE is a command issued by Master Monitor to Slave Monitor. Upon receiving SELECTIVE SANITIZE command Slave Monitor.

V. MALWARE DETECTION

Slave Monitor generates reports based on smart device behavior. Reports consist of data including but not restricted to bandwidth usage of devices, recognizable software list installed in the devices, memory usage. Master Monitor analyzes the report to find suspicious malware activity. Malware detection may be signature based or anomaly based. Signature based detection algorithms uses characteristics of what is known to be a malicious activity to inspect program maliciousness. Anomaly based malware detection algorithms distinguish between malicious behavior and *Safe state* behavior.

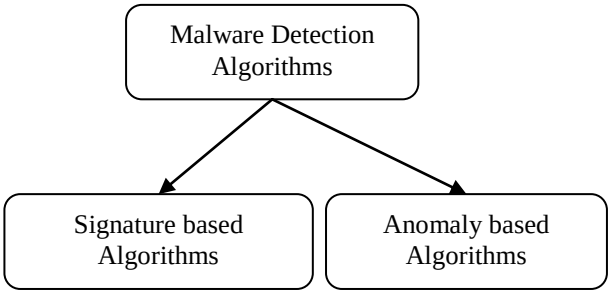

Figure 2: Classification of Malware detection algorithms

VI. RESULT AND CONCLUSION

Internet of things (IoT) increases connectivity and all the devices of our daily use may be destined to connect to internet and become smart devices [3]. If devices work correctly as predicted, they increase human comfort else they may harm the user if they behave abnormally. With IoT evolving, more focus should be on security of smart devices. Malwares which get injected into smart devices may harm the user by different measures. The monitoring system proposed in this paper, where slave monitors which dynamically reports to master monitor and executes commands issued by master monitor, can be used to detect and take necessary actions on malwares. Making monitoring system more intelligent is the future scope of this research.

REFERENCES

[1] http://www.internetsociety.org
[2] http://www.wired.com
[3] http://www.cisco.com