Summer Training Project Report
Summer 2017

Smart Home Benchmark Application

Faculty advisor: Brian Demsky Professor
UNIVERSITY OF CALIFORNIA, IRVINE
The Henry Samueli School of Engineering
Department of Electrical Engineering and Computer Science

Graduate Mentors: Rahmadi Trimananda, Ali

Undergraduate Researchers : Janghoi Koo
UNIVERSITY OF HANYANG
Department of Computer Science
Dohyon Kim
UNIVERSITY OF HANYANG
Department of Computer Science

Abstract

With the development of IoT[1] technology in these days, it is getting closer to the day when Smart Home will become our daily life. But because of ‘excessive network’ problem in The Smart Home[2], Users are more likely to be exposed to network attacks. This is because each device is allowed to communicate with other devices or even with other systems without any firewall protection.This project uses the Sentinel System and the Fidelius protocol to solve these Network security problems.The Sentinel System uses a strict routing policy that limits excessive network access and minimizes the attack surface of smart home IoT systems. Also the Fidelius protocol use a ‘Key-Value’ store method to securely send and receive information. Eventually, the researchers are creating a smartphone application that safely controls the Smart Home.This architecture is enabled by communicating between the app and the Sentinel, centered on the cloud server using the Fidelius protocol. So, The Smart home can be protected from malicious network attacks and it has been proved that negligible overhead occurs in this process.

---

[1] **The Internet of Things (IoT)** is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivitywhich enable these objects to collect and exchange data.[1][2][3] https://en.wikipedia.org/wiki/Internet_of_things

[2] **Smart Home** is the term commonly used to define a residence that has appliances, lighting, heating, air conditioning, TVs, computers, entertainment audio & video systems, security, and camera systems that are capable of communicating with one another and can be controlled remotely by a time schedule, from any room in the home, as well as remotely from any location in the world by phone or internet. http://www.smarthomeusa.com/smarthome/

Introduction

The IoT technology has been developing rapidly and is changing our lives. These IoT technologies are applied to household appliances and other equipment to make our lives easier. For example, a sensor attached to an air conditioner can control the temperature of the house from the outside. These are called smart homes. Although smart homes have not been universal yet, in the near future we will surely live in a smart home. However, this smart home has several security vulnerabilities because the sensors are designed without worrying about network security and each sensor is over-privileged without any restriction on communication with other sensors. This vulnerabilities can be used for malicious network attacks, for example, a malicious hacker can steal a camera in the house by hacking through the network. Therefore, this research was conducted to safeguard and control smart home against such network attacks. To protect smart home from these network attacks, the researchers developed an application that uses a secure protocol[3] to communicate with a smart home which is composed of Sentinel System[4]. In addition, the researchers have added several functions to the Sentinel System to ensure greater security. This paper explains how this process works.

---

[3] In telecommunications, a **communication protocol** is a system of rules that allow two or more entities of a communications system to transmit information via any kind of variation of a physical quantity. The protocol defines the rules syntax, semantics and synchronization of communication and possible error recovery methods. Protocols may be implemented by hardware, software, or a combination of both.[1]

[4] **The Sentinal system** is a previously studied system by professor Demsky that isolates communications by instating installer specified permissions as firewall rolls at router to out of insecure components. (designed to protect an IoT system from security issues resulting from overprivileged network access.)

Methods and Materials

Researchers use three major methodologies in this project, the first is the Sentinel System. As explained before, the network vulnerability of smart home is caused by the problem of communication between sensors. This is because communication between the sensors is more than necessary(excessive) and there are no firewall rules. Therefore, the researchers overcome these problems by using the Sentinel System. A Sentinel System is a way to limit excessive communication between sensors and isolate the system from unstable network access using strict routing policies.

In this research, three sensors (motion sensor, multi-purpose sensor, water-leak sensor) and camera constitute a smart home within the sentinel system, and when each device detects an abnormal state, it will trigger an alarm system to inform the user.

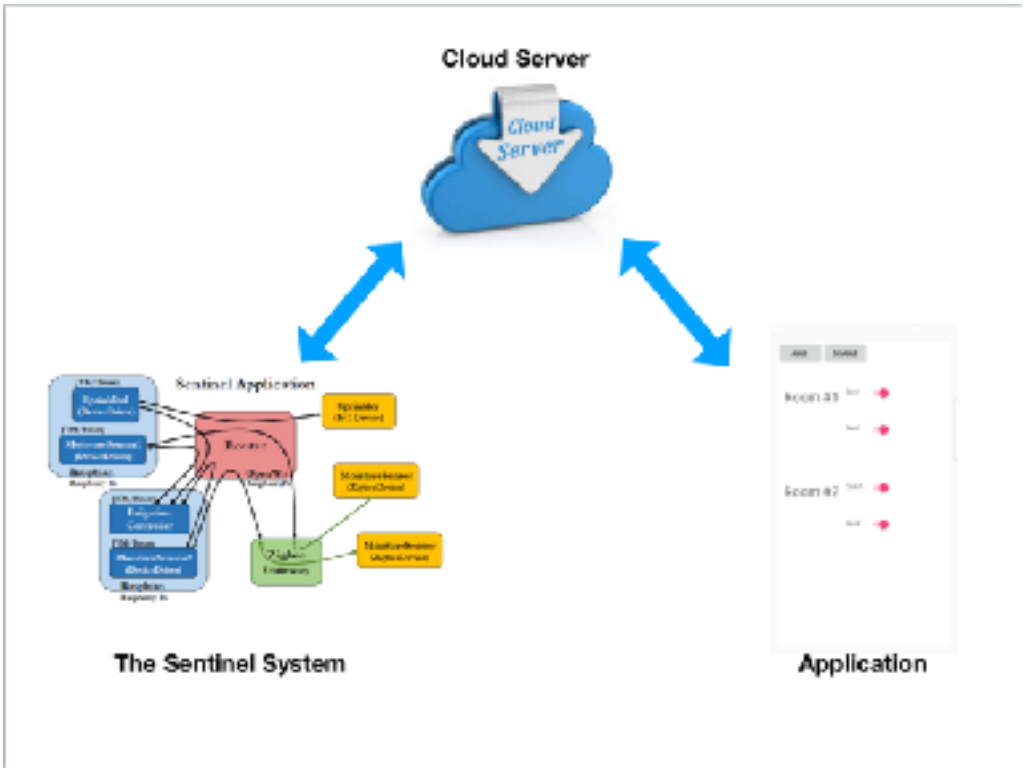
The second is the Cloud server. the researchers use the cloud server as an intermediary between the application and the smart home for blocking unauthorized access. This blocking mechanism was implemented using the Fidelius protocol, which is the third methodology.

Researchers use this protocol to allow applications to securely control the smart home, which is the key-value store method to securely send and receive information. In other words, the Fidelius protocol allows you to securely store keys and values in a cloud server by sharing a secret key that can decrypt and authenticate messages. For example, if a key for whether a single camera detects a threat can be 'cam1_detect' and a value can be 'true' or ‘false’. So, the application and the sentinel will be able to communicate through the cloud server secretly sharing the key and value. These mechanisms can be assured of security against improper access.

Using these three methods, researchers added three functions to the application. The first function is to allow the user to ignore specific sensors. For example, if the user is cooking late at night, the user can ignore motion sensor in the kitchen. The second function is to enable or disable the alarm system. For example, when the user leaves the house , the user can enable whole alarm system. and disable the alarm system if many guests are invited to the house. The third function is ‘monitoring’. that is a notifications to the smart phone when the alarm is triggered. It also tells you which sensor have triggered the alarm.

Results

The overall structure is like below.



The application and The Sentinel System communicate with each other. Through this process, using the Fidelius protocol, the smart home is protected against network attacks. Eventually the user can securely control the smart home through the application.

Discussion

Fundamental principles of sentinel systems which is ‘Router-based policy checking’ is not a new idea and it has been extensively studied in the software-defined networking (SDN) community. In addition, most smart home devices are universal. So, It does not communicate with any computer and does not require full network access. Therefore, it has been demonstrated in previous studies that limiting unnecessary communications has no significant impact on the overall system performance and incurs negligible runtime overhead.This study focused on this point.

Finally, this study does not defend against hardware hacking because it is intended to defend against software and network attacks.