Internet of Things Devices

Prepared by/

Table of content:

Abstract

We present our continuing work on SPIN, which is the more important and needed open source measurement platform that makes and allows investigators and the users to hardly study and analyze the security features of the devices in the "Internet of Things" (IoT), precisely in-home networks.

SPIN accomplishes this by mapping and enhancing network-level measurements in the home network and making them offered through a well-defined interface. This enables all the types of new applications for research and commercial reasons, such as privacy managers for consumers that visualize insecure IoT devices and their connections, and new algorithms that automatically block botnet traffic to protect the public Internet against IoT-powered DDoS attacks. SPIN is a supple distributed system which runs in the home network and it keeps users in the control. We have confirmed SPIN in our lab through prototype applications.

INTRODUCTION

The “Internet of Things” (IoT) is a term which typically goes back for connecting a large number of assorted objects to the Internet. Devices which are used are gradually becoming keener through adding processing power and a network connection for them. For fridges, door locks, baby monitors, and light bulbs.

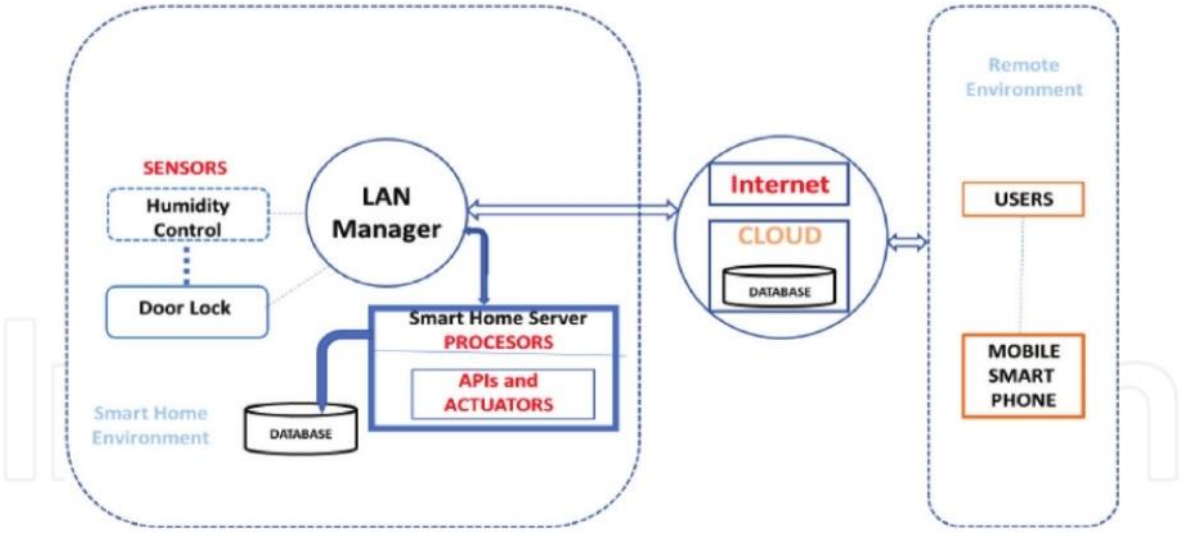
Although the IoT can help people in their daily lives, also it can expose their security, privacy, and safety because IoT devices are often unconfident; for example devices used in home networks like baby monitors that remote adversaries can exploit to reroute its video feed, devices like a vacuum cleaner that dynamically build up an indoor map of a house and silently shares it with the device’s manufacturer for good purposes also devices with programming errors that render the device inoperable that result in a shutdown of all communications within a house.

In addition to this user dangerous, the IoT poses a large-scale security threat to the Internet because it's insecure, compromised IoT devices enable are massive which attacks can broke and shut down parts of the Internet. This was typified by the Oct 2016 DDoS attack on DNS provider Dyn ,that was carried out by an estimated 100,000 IoT devices infected with the Mirai botnet and led to outages of popular services like Twitter. Consumers are unlikely to be interested in such attacks as they do not know the

The main mechanisms of IoT:

The main mechanisms which allow all of the above described activities and data management are in system, and the system is consisting of the following components

In the below figure it is shown Sensors to collect internal and external home data and measure home conditions. These sensors are linked to the home and to the attached home devices. These sensors are not internet of things sensors, that are attached to home appliances. The sensors' data are collected and repeatedly transferred via a local network, to a smart home server which Processes for performing local and integrated actions. It may also be connected to the cloud for applications requiring extended resources. The sensors' data is then processed by the local server processes. The collection of software components wrapped as APIs, allowing external applications in order to execute it, given it follows the pre-defined parameters format. Examples of an API can process sensors data or manage necessary actions.



The advantages and good points about IoT:

1. IoT can turn on and turn off the LED lights and also screen the condition of the LED.
2. It can bolt and open the entryways by the way of servo engines and screen in case of the entryways are bolted or opened.
3. It can screen if the entryways are shut or opened through IR sensors.
4. It is advised by email if the entryway is left open for a really long time.
5. It is advised of who entered through the entryway as the camera catches the face picture and send it to him/her by means of email.
6. It is cognizant through email if the fire identifier feels smoke.
7. It is ready to control the observation vehicle from anyplace to screen.

The Structure of Internet of Things:

A smart home can be identified by a residence which is fortified with clever items, a home community can make it possible to transfere records between items and a residential gateway to link and attach the clever domestic to the outdoor net world. Clever items make it feasible to have interaction with inhabitants or to study them. Technically, home Automation system are consisting of 5 building blocks.

- Devices under Control

These devices contain all the additives, and consisting of domestic home equipment or client electronics, that are related managed through a home automation device.

- The Sensors and Actuators

Sensors can study, hear and watch, within the domestic system. There are sensors for a broad collection of employs, such as, estimating temperature, light, fluid, moistness and fuel also figuring out development or commotion. Actuators are the strategies for the eager system can in all fact get matters carried out in fact. There are mechanical actuators, for example siphons and electrical engines or digital actuators. A system with each the sensors and actuator will see and carry out.

- Architecture

The authors present a layer architecture model of smart home control system based on Internet of Things which consists of Perception Layer, Network Layer and Application Layer.

SPIN CONCEPT

In the below Figure it shows the SPIN concept for a simple home network that consisting of two light bulbs which are a thermostat and a smart window. The light bulbs connect to the home network by network bridge because they use Zigbee as their link-level protocol.

The thermostat and the smart window can also be linked to the network bridges and all three bridges connect to each other and to the Internet through the home router.

SPIN's task are protecting users and the Internet from vulner- able IoT devices and might also carry out the DDoS attacks through a large number of indicators on the Internet and amplifying the attack by requesting the reflectors to use responses which are much larger than the original ones.

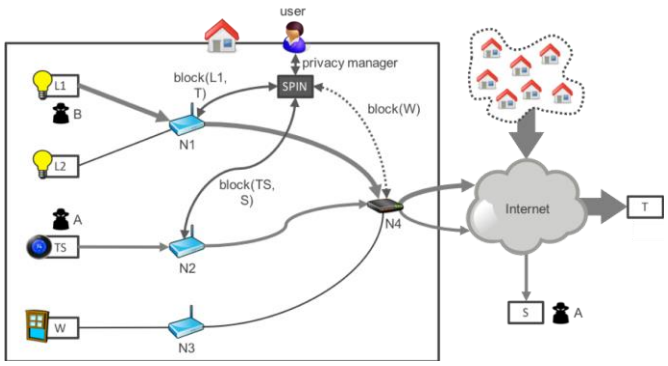
Through different ways we can comprome *TS* and *L1*, for example through (a weak) password guessing a same site scripting attack a DNS rebinding attack or by manipulating the device's access control list which might also misuse *L1* and *TS* for other reasons, such as getting the user credentials.

SPIN's privacy manager knows the user that *TS* is connecting to server *S*, which is different from *TS*' normal behavior.

The user then decides to block the outgoing flow instructs node *in order* drop packets from *TS* to *S*

In both cases, the user may contact a specialized service provider to help getting *L1* and *TS* to be cleaned, for instance by installing a new firmware version.

It also illustrates that the abilities of the nodes in a home network are differentwhich means the SPIN system can measure their traffic and block traffic flows passing through them.



THE DESIGN GOALS

We put four design goals for SPIN as shows below:

- To obtain a measurement tool for IoT security applications in home networks
- To allow for full in-home system deployment
- To control security and privacy at the network-level
- To make the user to be in control.

The Measurement API and SPIN Applications

We aim for SPIN to offer an easy measurement API which offers a high-level and longitudinal model of a home network and its IoT devices to application developers, making them to nonconcrete away from the particularities of device and network measurements.

Another goal is offering applications which are used the SPIN tool. We already built two applications which are:

The privacy manager which envisions the IoT devices on the network exhibit potentially suspicious behavior

The "reverse firewall" which mitigates IoT-powered DDoS attacks by an automatically blocking suspicious.

Network-level Control

We also aim for SPIN to provide the network-level security and privacy control. which means that SPIN analyzes network traffic and the generic security properties of IoT devices if you use another passwords or if they are susceptible to reflection attacks the blocks flows at intermediate network equipment, such as bridges and routers. SPIN therefore does not rely on IP packet payloads.

The advantages of a network-level security is generic and works for a wide range of IoT devices, that are important since the IoT devices are much more varied than personal computers and laptops.

Another advantage of network level is that the consumers can continue to use the IoT devices of their choice and they are not locked for using specific types of devices as those supported by their access provider.

User Control

Another design goal is for SPIN-based systems is to make the consumer to be control. for accomplish this task, we have to provide a central preference manager as a part of the SPIN system which enables the users to arrange their security and privacy control preferences

The 5 Types of IoT Wireless Technologies and uses:

1- Cellular

Cellular is one of the well-known type of IoT wireless technology it is particularly uses in the consumer mobile market. Cellular networks can offer a reliable broadband communication which helps everything from streaming applications to voice calls.

2- Bluetooth and Bluetooth Low Energy

Bluetooth is a well-known wireless technology in consumer circles. This wireless personal area network is a short-range communication technology with the optimization for power consumption; this is designed supporting small-scale consumer IoT applications.

3- WiFi

WiFi is playing a critical role in offering a high data transfer in homes, it's another well-known IoT wireless technology. It can have quite effective in the right situations, though it has significant limitations with scalability, coverage, and high power consumption. Due to newer enterprise security practices, IoT devices are discouraged from being added to the same primary Wi-Fi networks as phones and traditional employee computers.

4- LPWAN

Low power wide area networks provides long-range communication by using small, cheap batteries. This family of technologies are ideal for helping a large-scale IoT networks where a significant range is required. However, LPWANs can only send small blocks of data at a low rate.

5- LoRaWAN

LoRaWAN is one of the powerful and emerging technologies. This like Bluetooth, but it differs from Bluetooth in a way that this offers a longer range for small data packets with low power consumption. LoRaWAN achieves the communication frequencies, power, and data rate for all the connected devices.

What is the number one product that uses to control with home automation?

The number one product which is used by people is the one that is used in thier home and it is central heating and cooling.

As that temperature control accounts for the largest portion of energy use on a monthly basis, it's no surprise that a smart thermostat is the most common smart home device.

Why IoT is important in home automation?

You can control your devices like light, fan, TV, etc. In the IoT home automation ecosystem, A domestic automation system can monitor and/or manage home attributes adore lighting, climate, enjoyment systems, and appliances. It is very helpful to control your home devices

What are the best IoT projects for the beginners?

The Internet of Things is important for simplifying our daily life, it can be over systems that increase home comfort, traffic control, or environmental systems. A fan is a straightforward gadget, but when it connects to a smartphone to switch on and off, it transforms into a smart object or Internet of Things (IoT) object. We can develop this particular type of technology more to get benefits from it better.

The projects for the beginners are listed below:

- Home Automation System
- Weather Reporting System based on Raspberry pi
- Car Parking Management System
- Based Smart Agriculture System
- The Health Monitoring System
- Air & Noise Pollution Monitoring System

- Smart Street Light Monitoring System

- Night Patrol Robot
- Smart Garage Door

The major issues and problems of IoT:

All the aspects which are involved in human live and different types of technologies are have connection with the data transfer between the devices made which made it complex, there are a number of issues and challenges involves in this issue, the issues are listed below:

Security and privacy issues: this happens due to a number of threats, cyber-attacks and risks.

Interoperability issues: The interoperability issue arises due to the heterogeneous nature of different technology and solutions used for IoT development.

Ethics, law and regulatory rights: Another issue for IoT developers is the ethics, law and regulatory rights.

Scalability, availability and reliability: A system is scalable if it is possible to add new services, equipment's and devices without degrading its performance. The main issue with IoT is to support a large number of devices with different memory, processing, storage power and bandwidth.

Conclusions:

The main aim of this paper is giving short and brief information about the IoT based on Smart home Environments with an emphasis on their empowering progresses. An application zones, structures and designs. This objective isn't to give a point by point explanation for the subject, the peruse the fundamental standards and a short diagram of each subject, just as the list of sources to be checked in the event that somebody wishes to develop on certain parts of the subject.

The IoT will likely enable a wide range of new applications and services, but its large number of insecure devices also postures a danger to the user's privacy and the stability of Internet. In order to solve this issue, researchers and companies need flexible measurement platforms for home networks that enable them to easily develop and evaluate new IoT security applications, such as privacy management applications for consumers and new anomaly discovery algorithms.

We think that SPIN is a distributed system that can be flexibly deployed in a wide range of home networks and provides applications with an easy-to-use measurement-based data model of the network’s IoT devices and their security features.

References:

- M. Garrett. (2016, Feb).
- A. Barth, C. Jackson, and J. C. Mitchell,"Robust defenses for cross-site request forgery," *Proceedings ACM conference on Computer and communications security.*
- C. Jackson, A. Barth, A. Bortz, W. Shao, and D. Boneh, "Protecting browsers from dns rebinding attacks 2007.
- Mehani, "Network-level security and privacy control for smart-home IoT devices," 2015
- Cisco. (2019, Nov) Snort - network intrusion detection and prevention system.
- E. Leverett, R. Clayton, and R. Anderson, "Standardisation and certification of the 'internet of things'," June 2017.
- Frank Greer/ July 12th 2021/ zipitwireless.com