Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)

Кафедра Інфокомунакаційної інженерії імені В.В.Поповського
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Аналіз підходів забезпечення конфіденційності та безпеки в Інтернеті речей

An analysis of privacy and security approaches in the Internet of Things
(тема)

Виконав:
студент 2 курсу, групи АМСЗІмі-18-1
Булаід Айюб
(прізвище, ініціали)

Спеціальність: 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми: освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма: Адміністративний менеджмент у сфері захисту інформації
(повна назва освітньої програми)

Керівник: доцент кафедри ІКІ ім. В.В. Поповського
Радівілова Т.А.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2020 р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека
(код і повна назва)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма Адміністративний менеджмент у сфері захисту інформації
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
“____” _____ 20__ р.

ЗАВДАННЯ

НА АТЕСТАЦІЙНУ РОБОТУ

студентові Булаід Айюб
(прізвище, ім’я, по батькові)

1. Тема роботи: Аналіз підходів забезпечення конфіденційності та безпеки в Інтернеті речей.
затверджена наказом по університету“ 17 ” жовтня 2019 р.№ 348Ст
2.Термін подання студентом работи 25.12.2019
3. Вхідні дані до роботи методи захисту пристроїв Інтернету речей, протоколи взаємодії пристроїв, методи захисту безпечної передачі даних, уразливості мережі
Інтернету речей, методи аналізу захищеності пристроїв та мереж, методи
4. Перелік питань, що потрібно опрацювати в роботі
1) Кібербезпека та інформаційна безпека
2)Тестування на проникнення за допомогою засобу Kali Linux
3)Розробка інформаційної системи та її тестування на проникнення
4)Рішення задачі захисту корпоративної комп’ютерної мережі

5. Перелік графічного матеріалу із зазначенням креслеників, схем, ілюстрацій

Демонстраційний матеріал у вигляді ppt-презентації;опис актуальних вразливостей, засоби захисту від них; аналіз вразливостей за допомогою Penetration Testing

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		Підпис	дата
Основна частина	доцент Радівілова Тамара Анатоліївна		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	02.09.2019	Виконано
2	Збір матеріалів для дослідження	22.09.2019	Виконано
3	Розробка 1 розділу	29.09.2019	Виконано
4	Розробка 2 розділу	06.10.2019	Виконано
5	Розробка 3 розділу	13.10.2019	Виконано
6	Розробка 4 розділу	20.10.2019	Виконано
7	Оформлення атестаційної роботи	31.11.2019	Виконано

Дата видачі завдання 02 вересня 2019 р.

Студент Булаід Айюб
(підпис)(прізвище, ініціали)

Керівник роботи _____ Радівілова Т.А.
(підпис) (посада, прізвище, ініціали)

ABSTRACT

Thesis contains: 73 pages, 23 figures, 3 tables, 19 references.

DATAPLICITY, REMOTE MANAGEMENT, HOME AUTOMATION, IoT, RASPBERRY PI, WEB INTERFACE, SECURITY, PRIVACY

The object of study is the process of ensuring the safety of devices of the Internet of Things.

Subject of research is methods for identifying vulnerabilities when protecting devices that are connected to the Internet of Things from unauthorized access.

The purpose of the work is to analyze the vulnerabilities and methods of ensuring the confidentiality and security of the Internet of Things systems.

The main objectives of the study:

- analysis of information security requirements;
- security analysis of Internet of Things devices;
- modeling of attacks on methods of security of Internet of Things systems.

The work investigates vulnerabilities of the Internet of Things and analyzes the security of Internet of Things systems using Penetration Testing methods.

РЕФЕРАТ

Пояснювальна записка містить: 73 сторінок, 23 рисунків, 3 таблиць, 19 джерел.

DATAPLICITY, ВІДДАЛЕНЕ УПРАВЛІННЯ, ДОМАШНЯ АВТОМАТИЗАЦІЯ, ІНТЕРНЕТ РЕЧЕЙ, RASPBERRY PI, ВЕБ-ІНТЕРФЕЙС, БЕЗПЕКА, ПРИВАТНІСТЬ

Об`єкт дослідження – процес забезпечення безпеки пристроїв Інтернету речей.

Предмет дослідження – методи ідентифікації вразливостей при захисті пристроїв, що об’єднані в мережу інтернету речей, від несанкціонованого доступу.

Мета роботи – проведення аналізу вразливостей та методів забезпечення конфіденційності та безпеки систем Інтернету речей.

Основні задачі дослідження:

– аналіз вимог до забезпечення інформаційної безпеки;
– аналіз захищеності пристроїв інтернету речей;
– моделювання атак на методи забезпечення безпеки систем Інтернету речей.

У роботі проведено дослідження вразливостей мережі Інтернету речей, проведено аналіз безпеки систем інтернету речей за допомогою методів Penetration Testing.

Реферат

Пояснительная записка аттестационной работы: 73 с., 23 рис., 3 табл., 19 источников.

DATAPLICITY, УДАЛЕННОЕ УПРАВЛЕНИЕ, ДОМАШНЯЯ АВТОМАТИЗАЦИЯ, ИНТЕРНЕТ ВЕЩЕЙ, RASPBERRY PI, ВЕБ-ИНТЕРФЕЙС, БЕЗОПАСНОСТЬ, ПРИВАТНОСТЬ.

Объект исследования - процесс обеспечения безопасности корпоративных сетей.

Предмет исследования-методы идентификации уязвимостей в защите операционных систем, используемых в корпоративных сетях от несанкционированного доступа.

Цель работы -моделирование вероятности прохождения атак на различные операционные системы в корпоративных сетях.

Основные задачи исследования:

- анализ требований к обеспечению информационной безопасности;

- анализ защищенности современных операционных систем;

- моделирование атак на операционные системы и анализ уязвимых мест.

В работе виконено исследования уязвимостей информационной системы с помощью средств программного обеспечения KaliLinux.

Результаты работы докладывались на трех научных конференциях.

CONTENTS

LIST OF ABBREVIATIONS

ASCII	- American Standard Code for Information Interchange
ANSI	- American National Standards Institute
CSMA/CD	- Carrier Sense Multiple Access with Collision Detection
FTP	- File Transfer Protocol
HTTP	- Hypertext Transfer Protocol
IP	- Internet Protocol
IoT	- Internet of things
IEEE	- Institute of Electrical and Electronics Engineers
LAN	- Local Area Network
MAC	- Media Access Control
OSI	- Open System Interconnection
PoC	- Proof of concept
PPP	- Point-to-Point Protocol
ROI	- Return on investment
RFC	- Remote Function Call
SMTP	- Simple Mail Transfer Protocol
SSL	- Secure Socket Layer protocol
XSS	- Cross Site Scripting
TCP/IP	- Transmission Control Protocol / Internet Protocol
TP4	- Transmission Protocol - Class 4 protocol
VoIP	- Voice over Internet Protocol
VLAN	- Virtual local area networks
WAN	- Wide Area Network
Wi-Fi	- Wireless Fidelity

INTRODUCTION

The Internet of Things is the most trending technology today. The concept is simple: Your Home/industrial appliances/sensors in your home, office (or wherever you are) have the ability to communicate with each other via the internet. This technology often uses sensors to communicate data to the internet. To be simple, sensors are installed in your living-room, uploads data: as temperature, humidity, and light detection; to the internet, and this data is sent to you from anywhere in the world. Or we can imagine a home automation system we can use to control appliances in our home like lights, door locks, and air conditioning through a web interface or a smartphone application. A lot of technologies are being developed around this concept, such as independent IoT networks and protocols for passing data.

The portability and technologies of smartphone increased the user's interest in controlling their appliances from smartphones. The automated appliance control enables users to do tasks before arriving home. Users may not be prepared for their roles in our digital future, in which individual acts can affect communities and enterprises. Basic cyber education must be prioritized by businesses, and consumers.

This highly interconnected network as we call as Internet of Things will change everyone's life, increase business productivity, improve government efficiency, and the list is long. However, this new network system (IoT) is built on the basis of Internet, contains new type of challenges from a security and privacy perspective. Traditional security cannot be directly applied to IoT technologies because of the different standards and communication network and technologies involved. Along with this mix of standards and protocols issues, major part of IoT infrastructure consists of resource devices such as RFIDs and wireless sensor nodes. That's why a homogenic infrastructure is needed to deal with security and privacy issues in such an un-normalized environment.

This paper presents an overview of IoT, security and privacy challenges and the current and future security solutions and identifying some open issues for future research.

Recent cyberattacks like WannaCry, Petya, and much more illustrate why a combination of end user education and end-point security is important. WannaCry and Petya victims used outdated and unpatched versions of operating systems, which is a lesson in the importance of upgrading and patching devices.

The Internet of Things (IoT) is a revolutionary concept, however, with this great evolution comes various challenges that threatens the information technology industry these of course include security and privacy issues.

If one thing can prevent the Internet of things from transforming the way we live and work, it will be a breakdown in security. While security considerations are not new in the context of information technology, the attributes of many IoT implementations present new and unique security challenges. All more urgent is a clear understanding of the issues we confront and how they can be solved in order to fully use this capability.

1 IoT OVERVIEW AND BACKGROUND

The idea of connecting '*things*' to the internet extends much further back than the use of the term 'Internet of Things'. *In the early 1980s students at Carnegie Melon University fitted internet-connected photo sensors to a soft drink vending machine, which allowed them to count the number of cans that were being dispensed. This enabled anyone has access to the internet to determine how many drinks had been dispensed, and thus how many were remaining (Vetter 1995).*

Even before the first webpage was created, John Romkey and Simon Hackett introduced a toaster that was connected to the internet in 1990. Romkey's presentation at the 1990 Interop Conference featured an internet-connected Sunbeam Deluxe Automatic Radiant Control toaster, and arose as the result of a challenge at the previous year's conference from Dan Lynch, President of Interop, to Romkey. Lynch had promised Romkey centre stage at the event if he succeeded. The toaster was connected using TCP/IP and had a Simple Networking Management Protocol Management Information Base (***SNMP MIB***) controller; it's one function was to turn the power on or off. The first use of the term '***Internet of Things'*** came much later, and is widely attributed to Ashton (Ashton 2009), when he used it as the title of a presentation at Procter and Gamble in 1999.

There has been rapid growth in the number of devices connected to the internet. A number of analysts, notably Cisco and Ericson (Dave Evans and Hans Vestburg, respectively), have predicted that there will be 50 billion devices connected to the internet by 2020. Of course, these estimations are difficult to confirm with confidence, and both have now revised their estimates down. Evans, now at Stringify, predicts 30 million while Ericson estimates 28 billion by 2021.

One reason that it is difficult to predict growth is not only is there a great difference in figures using the same definitions, but the issue concerning the varying interpretations of the term IoT. Some clearly state the difference between machine-to-machine (M2M) and IoT devices, such as those of the GSMA, whose analysis of M2M focuses on cellular M2M connectivity and excludes computing devices in consumer electronics such as smartphones, e-readers, tablets, as well as other types of M2M connection technologies that support the wider universe of the Internet of Things (IoT).

A 2015 report by Machine Research predicted that the total number of M2M connections will grow from 5 billion in 2014 to 27 billion in 2024 (Machina 2015). Nordrum (2016) observed that, in 2016, Gartner estimated that there were 6.4 billion devices (excluding smartphones, tablets, and computers), the International Data Corporation estimated 9 billion (with the same exclusions) and IHS estimated 17.6 billion (including smartphones, tablets, and computers). A similar study by Juniper Research estimated that there were 16 billion devices.

While there are not exact numbers of connected IoT devices, it can be easily noticed that the number of devices is enormous, and growth has been, and is predicted to be, phenomenal. The Internet of Things is connecting more devices every day, and we're headed for a world that will have 64 billion IoT devices by 2025.

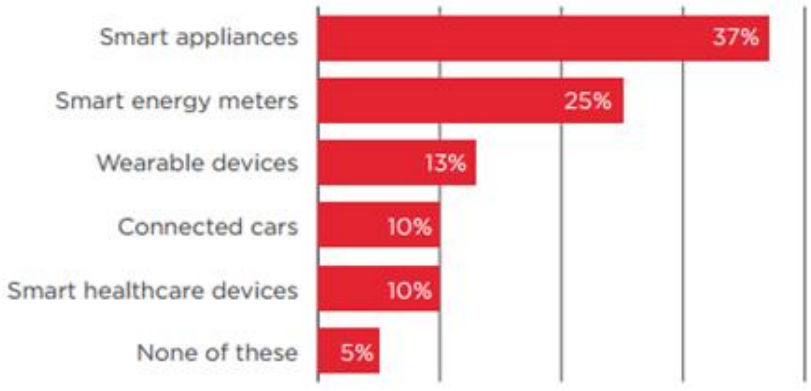


Figure 1.1 – IoT application showed by percent

This growth carries several benefits, as it will change the way people carry out daily tasks and potentially transform the world. Having a smart home is undoubtedly cool, but smart lighting can actually reduce overall energy consumption and lower your electric bill.

New developments allow connected cars to link up with smart city infrastructure to create an entirely different ecosystem for the driver, who is simply used to the traditional way of getting from Point A to Point B. And connected healthcare devices give people a deeper and fuller look at their own health, or lack thereof, than ever before.

But with all of these benefits comes risk, as the increase in connected devices gives hackers and cyber criminals more entry points.

Late last year, a group of hackers took down a power grid in a region of western Ukraine to cause the first blackout from a cyber-attack. And this is likely just the beginning, as these hackers are looking for more ways to strike critical infrastructure, such as power grids, hydroelectric dams, chemical plants, and more.

1.1 Application Areas of Internet of Things

The 10 most popular IoT applications are summarized by: applications for smart home, wearables, smart city, smart grids, Industrial internet, connected car, connected health (digital health / telehealth / telemedicine), smart retail, smart supply chain and smart farming (see reference [3]).

Security and privacy issues should be addressed to operate these systems and platforms.

1.1.1. Smart Homes, buildings, and offices:

Whenever we think of IoT systems, the most important and efficient application that stands out is the smart home, ranking the highest IoT application [1] on all channels. The number of people searching for smart homes increases every month by about 60,000 people. Another interesting thing is that the database of smart homes for IoT analytics includes 256 companies and start-ups. More companies are now actively involved in smart homes, as well as similar applications in the field. The estimated amount of funding for smart home start-ups increased $2.5 billion and growing at a rapid rate. The list of start-ups includes prominent start-up company's names, such as AlertMe or Nest, as well as a number of multinational corporations, like Philips, Haier, or Belkin.

1.1.2. Wearables: Health, well-being, and recreation:

Just like smart homes, wearables remain a hot trending topic among IoT. Every year, consumers all across the world wait the release of the latest Apple smartwatch and such concurrent products.

Apart from this, there are plenty of other wearable devices that make our life easy, such as the Sony Smart B Trainer, LookSee bracelet, Google Glasses, or the Myo gesture control.

1.1.3.Smart City

Smart cities, like its name suggests, is a big innovation and spans a wide variety of use cases, from water distribution and traffic management to waste management and environmental monitoring. The reason why it is so popular is that it tries to remove the discomfort and problems of people who live in cities. IoT solutions offered in the smart city sector solve various city-related problems, comprising of traffic, decreasing air and noise pollution, and helping to make cities safer.

1.1.4 Smart Grids

Smart grids are another area of IoT technology that stands out. A smart grid basically promises to obtain information on the behaviors of consumers and electricity suppliers in an automated fashion to improve the efficiency, economics, and reliability of electricity distribution. 41,000 monthly Google searches is a testament to this concept's popularity.

1.1.5 Industrial internet

One way to think of the Industrial Internet is by looking at connected machines and devices in industries such as power generation, oil, gas, and healthcare. It also makes use of situations where unplanned downtime and system failures can result in life-threatening situations. A system embedded with the IoT tends to include devices such as fitness bands for heart monitoring or smart home appliances. These systems are functional and can afford ease of use but are not reliable because they do not typically create emergency situations if a downtime was to occur.

1.1.6 Connected cars

Connected car technology is a vast and an extensive network of multiple sensors, antennas, embedded software and technologies that assist in communication to navigate in our complex world. It has the responsibility of making decisions with consistency, accuracy, and speed. It also has to be reliable. These requirements will become even more critical when humans give up control of the steering wheel and brakes to the autonomous vehicles that are being tested on our highways right now.

1.1.7 Connected Health (Digital health/ Telehealth/ Telemedicine)

IoT has big variety applications in healthcare, which are from remote monitoring equipment to advance and smart sensors integration. It has the potential to improve how physicians deliver care and also keep

patients safe and healthy. Healthcare IoT can let patients to spend more time interacting with their doctors, which can boost patient engagement and satisfaction. From personal fitness sensors to surgical robots, IoT in healthcare brings new tools updated with the latest technology in the ecosystem that helps in developing better healthcare.

IoT helps to revolutionize healthcare and provide pocket-friendly solutions for both the patient and healthcare professional.

1.1.8 Smart Retail

Retailers have started adopting IoT solutions and using IoT embedded systems across a number of applications that improve store operations, increasing purchases, reducing theft, enabling inventory management, and enhancing the consumer's shopping experience. Through IoT physical retailers can compete against online challengers more strongly. They can regain their lost market share and attract consumers into the store, thus making it easier for them to buy more while saving money.

1.1.9 Smart supply chain

Supply chains have already been getting smarter for a couple of years. Offering solutions to problems like tracking of goods while they are on the road or in transit station or helping suppliers exchange inventory information.

With an IoT enabled system, factory equipment that contains embedded sensors communicate data about different parameters, such as pressure, temperature, and utilization of the machine. The IoT system can also process workflow and change equipment settings to optimize performance.

1.1.10 Smart farming

Smart farming is an often overlooked in IoT applications. However, because the number of farming operations is usually remote and the large number of livestock that farmers work on, all of this can be run by the Internet of Things and can revolutionize the way farmers operate.

But this idea is yet to reach a large-scale attention. Nevertheless, it still remains one of the IoT applications that should not be underestimated. Smart farming has the potential to become an important application field, specifically in the agricultural-product exporting countries.

Figure 1.2. The four layers of IoT architecture described in detail

1.2 How an IoT system actually works:

The applications for IoT extend across a variety of use cases. However, all complete IoT systems are the same in that they represent the integration of four distinct compartments.

First of all, it consists of the Things, which are objects connected to the Internet which by means of their embedded sensors and actuators are able to sense the environment around them and collect information that is then passed

on to IoT gateways. The next stage consists of IoT data acquisition systems and gateways that collect the great mass of unprocessed data, convert it into digital streams, filter and pre-process it so that it is ready for analysis. The third layer is represented by edge devices responsible for further processing and enhanced analysis of data. This layer is also where visualization and machine learning technologies may step in.

After that, the data is transferred to data centers which can be either cloud-based or installed locally. This is where the data is stored, managed and analyzed in depth for actionable insights.

1.2.1 Sensors / Devices

A thing in the context of "Internet of Things", should be equipped with sensors and actuators giving the ability to emit, accept and process signals.

First, sensors or devices collect data from their environment. This data could be as simple as a temperature reading or as complex as a full video feed.

We use "sensors/devices/actuators" because multiple sensors can be bundled together or sensors can be part of a device that does more than just sense things. For example, your phone is a device that has multiple sensors (camera, accelerometer, GPS, etc.), but your phone is not just a sensor since it can also perform various actions.

However, whether it's a standalone sensor or a full device, in this first step data is being collected from the environment by *something*.

1.2.2 Data Acquisition Systems

Next, that collected data is sent to the cloud, but it needs a to connect

The sensors/devices can be connected to the cloud through a variety of methods including: cellular, satellite, Wi-Fi, Bluetooth, low-power wide-area networks (LPWAN), connecting via a gateway/router or connecting directly to the internet via Ethernet

Each option has pluses and minuses among power consumption, range, and bandwidth. Choosing which connectivity option is best comes down to the specific IoT application, but they all accomplish the same task: getting data to the cloud.

1.2.3 Edge Analytics

Once IoT data has been aggregated, it may require further processing before it enters the data center, this is where Edge Analytics comes in.

Software performs some sort of processing on it. This could be very simple, such as checking that the temperature reading is within an acceptable range. Or it could also be very complex, such as using computer vision on video to identify objects (such as intruders on a property).

1.2.4 User Interface

Data that needs more in-depth processing gets forwarded to physical data centers or cloud-based systems.

Next, the information is made useful to the end-user in some way. This could be via an alert to the user (email, text, notification, etc). For example, a text alert when the temperature is too high in the company's cold storage.

A user might have an interface that allows them to proactively check in on the system. For example, a user might want to check the video feeds on various properties via a phone app or a web browser.

However, it's not always a one-way street. Depending on the IoT application, the user may also be able to perform an action and affect the

system. For example, the user might remotely adjust the temperature in the cold storage, and/or some actions are performed automatically. Rather than waiting for you to adjust the temperature, the system could do it automatically via predefined rules. Rather than just call you to alert you of an intruder, the IoT system could also automatically notify security teams or relevant authorities.

2 PROTOCOLS IN IoT

At a time, when the number of Internet of Things (IoT) devices is continuously increasing, cases of DDoS (Distributed Denial of Service) attacks are also being witnessed at frequent intervals. Gartner reports that in 2020, the number of IoT devices will approximately reach 25 billion. It means that it is time when businesses, customers, and any enthusiasts should know about the IoT protocols and standards, which can potentially leave possibilities of security breaches.

IoT communication protocols are modes of communication that protect and ensure security to the data being circulating between linked devices.

The IoT devices are typically connected to the Internet via an IP (Internet Protocol) network. However, devices such as Bluetooth and RFID allow IoT devices to connect locally. In these cases, there's a difference in power, range, bandwidth and memory used. Connection through IP networks are comparatively complex, requires increased memory and power from the IoT devices while the range is not a problem. On the other hand, non-IP networks demand comparatively less power and memory but have a range limitation.

As far as the IoT communication protocols or technologies are concerned, a mix of both IP and non-IP networks can be considered depending on usage.

As stated previously, IoT architecture may vary from solution to solution, but the principle consists of the four building blocks that are key in providing the basic features that make an IoT ecosystem: Functionality, Scalability, Availability, Maintainability and cost-effectiveness.

We all agree that it is true that there are still a long road to be achieved in terms of overcoming IoT technology fragmentation, it is quite evident that much

research has been done to date to integrate the vast range of technologies and standards embraced by IoT (examples: LwM2M, oneM2M) and there is hope for a more unified and standardized in future.

However, before this comes true, the key to making the promise of IoT happen doesn't necessarily rely in obtaining a single rule-them-all IoT technology.

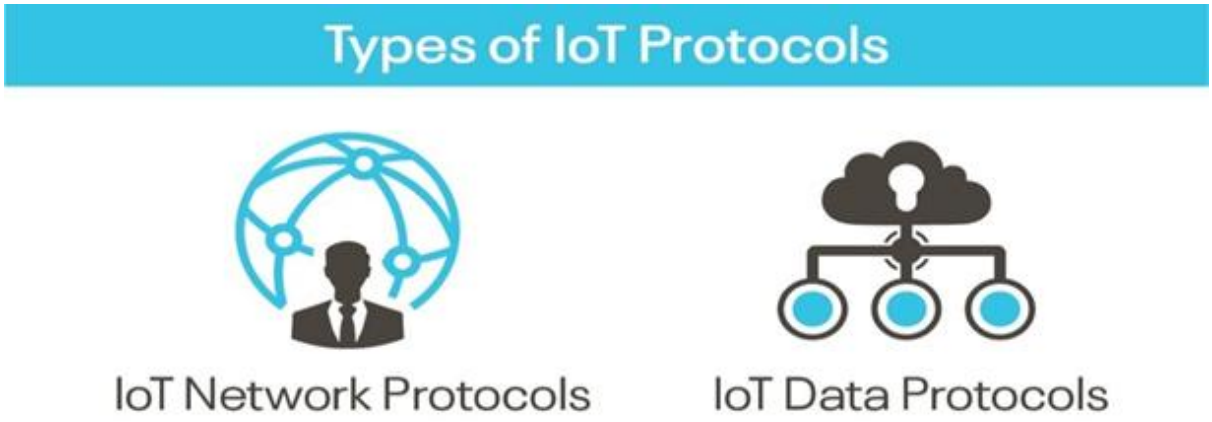


Figure 2.1. IoT protocols and standards can be broadly classified into two separate categories

2.1 IoT Network Protocols:

IoT network protocols are used to connect devices over the network. These are the set of communication protocols typically used over the Internet. Using IoT network protocols, end-to-end data communication within the scope of the network is allowed. Bellow there are the various IoT Network protocols:

2.1.1 HTTP (HyperText Transfer Protocol)

HyperText Transfer Protocol is the best example of IoT network protocol. This protocol has formed the creation of data communication over the web. It is the most common protocol that is used for IoT devices when there is a

lot of data to be published. However, the HTTP protocol is not preferred because of its cost, battery-life, energy saving, and more constraints.

Additive manufacturing/3D printing is one of the use cases of the HTTP protocol. It enables computers to connect 3D printers in the network and print three-dimensional objects and pre-determined process prototypes.

2.1.2 LoRaWan (Long Range Wide Area Network)

LoRaWAN is a WAN (Wide Area Network) protocol maintained by **LoRa Alliance**. It is a long-range low power protocol that provides signal detection below the noise level. It connects battery operated things wirelessly to the Internet in either private or global networks and it supports a secure bi-direction communication between IoT devices in M2M, smart cities and Industrial applications. Communications between IoT devices and gateway occurs at a different frequency and data rates.

This communication protocol is mainly used by smart cities, where there are millions of devices that function with less power and memory.

2.1.3 Bluetooth

Bluetooth is one of the most widely used protocols for short-range communication. It is a standard IoT protocol for wireless data transmission. This communication protocol is secure and perfect for short-range, low-power, low-cost, and wireless transmission between electronic devices. BLE (Bluetooth Low Energy) is a low-energy version of Bluetooth protocol that reduces the power consumption and plays an important role in connecting IoT devices.

Bluetooth protocol is mostly used in smart wearables, smartphones, and other mobile devices, where small fragments of data can be exchanged without high power and memory. Offering ease of usage, Bluetooth tops the list of IoT device connectivity protocols.

2.1.4 ZigBee

Another IoT network protocol that allows smart objects to work together is Zigbee. This is another wireless protocol widely used in WPAN. It is a standard maintained by **Zigbee Alliance**. Zigbee is commonly used in the smart energy area, and it is also used with security systems and in smart homes. ZigBee is built to save and reduce power consumption and mainly used with apps that support low-rate data transfer between short distances.

2.2 IoT Data Protocols:

IoT data protocols are used to connect low power IoT devices. These protocols provide point-to-point (P2P) communication with the hardware at the user side without any Internet connection. Connectivity in IoT data protocols is through a wired or a cellular network. Some of the IoT data protocols are:

2.2.1 Message Queue Telemetry Transport (MQTT)

One of the most preferred protocols for IoT devices, MQTT collects data from various electronic devices and supports remote device monitoring. It is a subscribe/publish protocol that runs over Transmission Control Protocol (TCP), which means it supports event-driven message exchange through wireless networks.

MQTT is mainly used in devices which are economical and requires less power and memory. For instance, fire detectors, car sensors, smart watches, and apps for text-based messaging.

2.2.2 Constrained Application Protocol (CoAP)

CoAP is an internet-utility protocol for restricted gadgets. Using this protocol, the client can send a request to the server and the server can send back the response to the client in HTTP. For light-weight implementation, it makes

use of UDP (User Datagram Protocol) and reduces space usage. The protocol uses binary data format EXL (Efficient XML Interchanges).

CoAP protocol is used mainly in automation, mobiles, and microcontrollers. It sends a request to the application endpoints such as appliances at homes and sends back the response of services and resources in the application.

2.2.3 Lightweight M2M (LwM2M)

OMA Lightweight M2M is a protocol from the Open Mobile Alliance for M2M or IoT device management. Lightweight M2M enabler defines the application layer communication protocol between a LwM2M Server and a LwM2M Client, which is located in a LwM2M Device. The OMA Lightweight M2M enabler includes device management and service enablement for LwM2M Devices. The target LwM2M Devices for this enabler are mainly resource-constrained devices. Therefore, this enabler makes use of a light and compact protocol as well as an efficient resource data model. It provides a choice for the M2M Service Provider to deploy a M2M system to provide service to the M2M User. It is frequently used with CoAP.

2.2.4 Advanced Message Queuing Protocol (AMQP)

AMQP is a software layer protocol for message-oriented middleware environment that provides routing and queuing. It is used for reliable point-to-point connection and supports the seamless and secure exchange of data between the connected devices and the cloud. AMQP consists of three separate components namely Exchange, Message Queue, and Binding. All these three components ensure a secure and successful exchange and storage of messages. It also helps in establishing the relationship of one message with the other.

AMQP protocol is mainly used in the banking industry. Whenever a message is sent by a server, the protocol tracks the message until each message is delivered to the intended users/destinations without failure.

2.2.5 Machine-to-Machine (M2M) Communication Protocol

It is an open industry protocol built to provide remote application management of IoT devices. M2M communication protocols are cost-effective and use public networks. It creates an environment where two machines communicate and exchange data. This protocol supports the self-monitoring of machines and allows the systems to adapt according to the changing environment.

M2M communication protocols are used for smart homes, automated vehicle authentication, vending machines, and ATM machines.

2.2.6 Extensible Messaging and Presence Protocol (XMPP)

The XMPP is uniquely designed. It uses a push mechanism to exchange messages in real-time. XMPP is flexible and can integrate with the changes seamlessly. Developed using open XML (Extensible Markup Language), XMPP works as a presence indicator showing the availability status of the servers or devices transmitting or receiving messages.

Other than the instant messaging apps such as Google Talk and WhatsApp, XMPP is also used in online gaming, news websites, and Voice over Internet Protocol (VoIP).

Over the last two decades, the Internet of Things has kept expanding rapidly over the globe. Having worked its way to numerous industry branches such as manufacturing, healthcare, automotive, security, transportation and more, it has significantly empowered enterprises and brought them economic value.

Today, the Internet of Things supports dozens of different IoT protocols. In view of this, many IoT experts have started to call for a global protocol standardization. Yet, being inherently fragmented, the IoT market will probably never be in actual need of an all-embracing standard. Just as there are newer and newer applications and use cases cropping up within the IoT industry, fit-for-purpose IoT protocols for their deployment will continue to emerge more and

more for the few upcoming years. Again, it should be emphasized that safe and effective device management is the keystone of a sustainable development of IoT networks worldwide.

This is one of the reasons why describing and making sense [17] of the various

Table 1. Communication technologies used in IoT and M2M systems

Communication technologies used in IoT and M2M systems.

Technology	Standard	Frequency	Coverage	Bit rate	Comments
WiFi	IEEE 802.11	2.4/5 GHz	50 m	500 Mbps	High consumption
ZigBee	IEEE 802.15.4	2.4 GHz	100 m	250 kbps	High security
Z-Wave	ZAD12837	900 MHz ISM	50 m	40 kbps	Home automation
Sigfox	Sigfox	900 MHz ISM	10 km	1 kbps	Low consumption
Neul	Neul	458 MHz	10 km	100 kbps	Low-cost IoT
LoRaWAN	LoRaWAN	ISM bands	15 km	50 kbps	Wireless battery operated IoT
RFID	ISO/IEC 18000	LF, ISM bands	<2 m	40 kbps	
NFC	ISO/IEC 18092	13.56 MHz	<20 cm	424 kbps	
GSM/3G/4G	GSM, UMTS/HSPA, LTE	900/1800/1900/2100 MHz	50 km	10 Mbps	High consumption
Bluetooth LE	IEEE 802.1	2.4 GHz	50 m	1 Mbps	Low consumption
6LoWPAN	RFC6282	ISM bands	n/a	n/a	
HomePlug	IEEE1901	<100 MHz	<100 m	10–500 Mbps	Smart grids
Thread	Based on IEEE802.15.4	2.4 GHz	<100 m	250 kbps	Up to 250 devices
DSRC	IEEE802.11p	5 GHz ISM	300 m	27 Mbps	V2V comms
WiMax	IEEE802.16	2.3, 2.5, and 3.5 GHz	10 km	10 Mbps	

IoT protocols really matters. Therefore, what is really needed is the knowledge of one’s own business needs and requirements, awareness of the advantages and drawbacks of the protocols offered by the market, and the ability to pick the one that best suits for each use-case.

3 SECURITY AND PRIVACY

As per an article published by Forbes, “approximately 32,000 smart homes and businesses are at risk of leaking data.”

Therefore, it becomes important to explore the potentials of IoT protocols and standards, which offers a secure environment. Using these protocols, local gateways and other connected devices so they could communicate and inter-change data with the cloud. This brings many benefits, as it will redefine the way people carry out every day’s tasks and potentially transform the world. For example, further developments would allow connected cars to link up with smart city infrastructure and create a whole new different ecosystem for the driver, who were before used to the traditional way of moving from Point A to Point B.

And connected healthcare devices give people a deeper and explicit report in real-time of their health.

But with all of these benefits comes risk, as the increase in connected devices gives hackers and cyber criminals more entry points, see Figure [4] and references [4].

Below, we've compiled a list of some of the biggest IoT security and privacy issues as we confront toward this truly wide connected world.

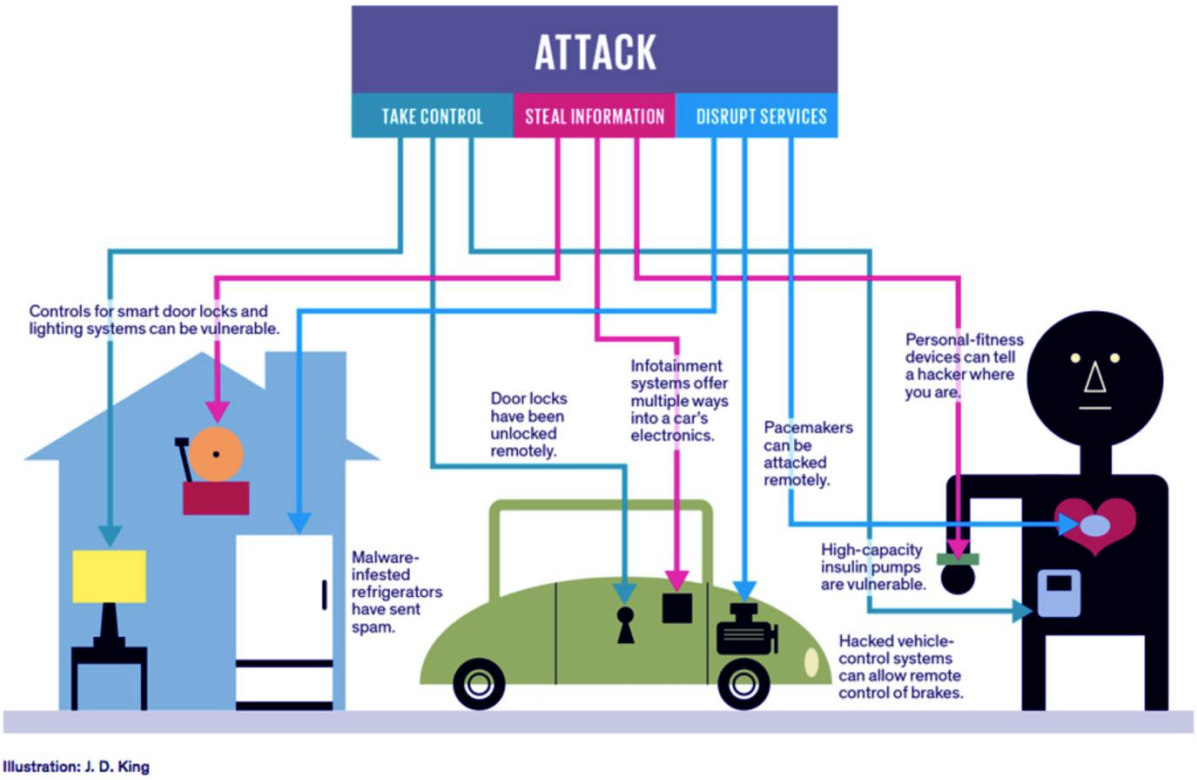


Figure 3.1. Explicit list of threats and security breaches in IoT

3.1 Security issues in IoT

As the IoT expands as well as it becomes an important asset of our critical national infrastructure, securing it must be vital. The securing of systems can be done following a multiple number of strategies, from the CIA of information security (confidentiality, integrity, and availability), to the five pillars of information assurance (confidentiality, integrity, availability, authenticity, and nonrepudiation) and the *Parkerian Hexad* (confidentiality, integrity, availability, authenticity, possession, and utility) (*Parker 1998*). Research articles discussing security considerations relating to cyber-physical (as opposed to information) and IoT systems vary in which principles they adopt.

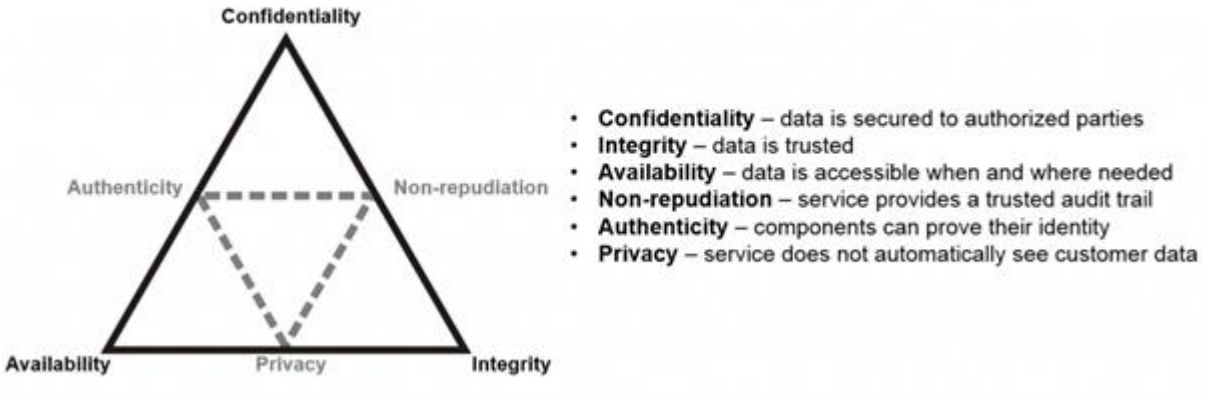


Figure 3.2 CIA Scheme

The majority of researchers restrict consideration to the CIA. The Parkerian Hexad, whilst originally offered as an improvement to overcome the limitations of the CIA [5], is often rejected; indeed, the usefulness of the Hexad remains the subject of debate among security professionals (Feruza and Kim 2007). Others go beyond these earlier principles and include robustness, reliability, safety, resilience, performability, and survivability (Sterbenz et al. 2010).

It is absolutely worth considering all of these components of security, especially in complex cyber-physical schemes like the IoT. However, for that part we use the three broadest categories of the CIA, understanding that the compromises may be of physical as well as information assets. We discuss some of the most significant challenges, highlighting which principles are under threat of breach and/or vulnerabilities. It must be recognized that this is not an exhaustive list of the security challenges.

To apply these security principles to the IoT, we need to define an IoT framework. For the purposes of this discussion we will divide the IoT into a simplified framework of three layers:

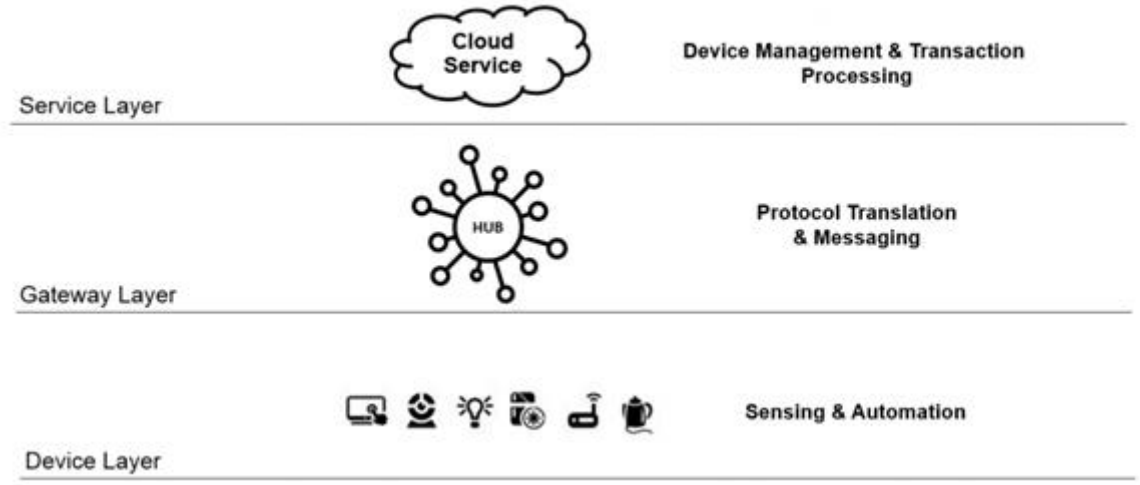


Figure 3.3 Security principles in IOT

3.1.1 Device layer:

This layer is like an intersection of people, places, and things. These things can be devices like connected TV and lightbulbs, or complex devices such as medical instruments and industrial equipment. For security in the IoT to be achieved, it must be designed and built into the devices themselves. To be simple; IoT devices must be able to prove their identity to maintain authenticity, sign and encrypt their data to maintain integrity, and limit locally stored data to protect privacy. The security model for devices must be strict enough to prevent unauthorized use, but flexible to support secure, ad hoc interactions with people and other devices on a temporary basis.

Because IoT devices will eventually exist everywhere in the environment, physical security is also important. This creates the need to think about a devices design so that it is difficult to extract sensitive information like personal data, cryptographic keys, etc. ... And, for sur, we think IoT devices to have long lives so it is important to enable software updates to prevent from the inevitable upcoming exploits that will be sure found one day.

3.1.2 Gateway layer:

The Gateway layer of the IoT framework represents the connectivity and messaging between things and cloud services. Communications in the IoT are usually over a combination of private and public networks, so securing the traffic is obviously important. This is probably the most understood area of IoT security, with technology like TLS/SSL encryption ideally suited to solve the problem. The primary difficulty arises when you consider the challenges of cryptography on devices with constrained resources, i.e. 8-bit microcontrollers with limited RAM. For example an Arduino Uno takes up to 3 minutes to encrypt a test payload when using RSA 1024 bit keys, however an elliptical curve digital signature algorithm (ECDSA) with a comparable RSA key length can encrypt the same payload in .3 seconds. This indicates that device manufactures cannot use resource constraints as an excuse to avoid security in their products.

Another security consideration for the gateway layer is that many IoT devices communicate over protocols other than Wi-Fi. This means the IoT gateway is responsible for maintaining confidentiality, integrity, and availability while translating between different wireless protocols, from Z-Wave or ZigBee to Wi-Fi for example.

3.1.3 Service layer:

This layer of the framework represents the IoT management system and is responsible for onboarding devices and users, applying policies and rules, and managing automation between devices. Role-based access control to manage user and device identity and the permissions they are authorized to make is importantly critical at this layer. To achieve non-repudiation, it is also important to maintain an audit trail of changes made by each user and device so that it impossible to refute actions taken in the system. This monitoring data could also

be a powerful tool to identify potentially compromised devices when abnormal behavior is detected.

Big data analysis of the aggregate data generated by IoT is often described as the most valuable aspect of IoT for device and service providers alike.

Many of the conversations taking place around the Internet of Things (IoT) are incomplete without a mention of big data. Connected devices, sensors, and algorithms all operate in ways that involve massive amounts of data.

"The success or failure of the Internet of Things hinges on big data," says Brian Hopkins, an analyst with Forrester Research. [12]

Inversely, maintaining consumer privacy is also top of mind for government agencies sharing their respective guidelines for securing the IoT. This creates a set of privacy rules related to security requirements such as: providing clear data use notification so that customers have visibility and fine grained control of the data sent to the cloud service, keeping customer data stored in the cloud service segregated and/or encrypted with customer provided keys, and when analyzing data in aggregate across customers, the data should be anonymized.

As we cited upper, there are many challenges to securing the IoT, many unique to each layer of the IoT framework. Robust security strategy starts by building it into the devices themselves. Even small resource devices in the IoT must implement cryptography to maintain confidentiality, integrity, and authenticity when communicating over the network.

Here is non-exhaustive enumeration of different type of attacks and their threat levels, nature and suggested solutions [11]:

Table 2. Various type of attacks, threat levels and suggested solutions

Type	Threat level	Behavior	Suggested Solution
Passive	Low	Usually breach data confidentiality. Examples are passive eavesdropping and traffic analysis. Hostile silently listen the communication for his own benefits without altering the data.	Ensure confidentiality of data and do not allow an attacker to fetch information using symmetric encryption techniques.
Man in the Middle	Low to Medium	Alteration and eavesdropping are the examples of this attack. An eavesdropper can silently sense the transmission medium and can modify the data if encryption is not applied and steal the information that is being transmitted. Hostile may also manipulate the data.	Apply data confidentiality and proper integration on data to ensure integrity. Encryption can be also applied so that no one can steal the information or modify the information or encode the information before transmission.
Eavesdropping	Low to Medium	The information content may be lost by an eavesdropper that silently senses the medium. For example in medical environment, privacy of a patient may be leaked.	Apply encryption on all the devices that perform communication.
Gathering	Medium to High	Occurs when data is gathered from different wireless or wired medium. Examples are skimming, tampering and eavesdropping. Data is being collected to detect messages. Messages may also be altered.	Encryption can be applied to prevent this kind of attack. Identity based method and message authentication code can also be applied in order to prevent the network from such malicious attacks.
Active	High	Effects confidentiality and integrity of data. Hostile can alter the integrity of messages, block messages, or may re-route the messages. It could be an internal attacker.	Ensure both confidentiality and integrity of data. To maintain data confidentiality, symmetric encryption can be applied. An authentication mechanism may be applied to allow data access to only authorized person.
Imitation	High	It impersonate for an unauthorized access. Spoofing and cloning are the examples of this attack. In spoofing attack a malicious node impersonate any other device and launch attacks to steal data or to spread malware. Cloning can re-write or duplicate data.	To avoid from spoofing and cloning attacks, apply identity based authentication protocols. Physically unclonable function is a countermeasure for cloning attack.
Privacy	High	Sensitive information of an individual or group may be disclosed. Such attacks may be correlated to gathering attack or may cause an imitation attack that can further lead to exposure of privacy.	Apply anonymous data transmission. Transmit sample data instead of actual data. Can also apply techniques like ring signature and blind signature.
Interruption	High	Affects availability of data. This makes the network unavailable.	Applying authorization, only authorized users are allowed to access specific information to perform certain operation.
Routing diversion	High	Only the route is diverted showing the huge traffic and the response time increased.	Ensure connectivity based approach so no route will be diverted.
Blocking	Extremely High	It is type of DoS, jamming, or malware attacks. It sends huge streams of data which may leads to jamming of network, similarly different types of viruses like Trojan horses, worms, and other programs can disturb the network.	Turn on the firewall, apply packet filtering, anti-jamming, active jamming, and updated antivirus programs in order to protect the network from such attacks.
Fabrication	Extremely High	Affects the authenticity of information. Hostile can inject false data and can destroy the authenticity of information.	Data authenticity can be applied to ensure that no information is changed during the transmission of data.
DoS	Extremely High	Malicious user may modify the packets or resend a packet again and again on network. User can also send bulk messages to devices in order to disturb the normal functionalities of devices.	Apply cryptographic techniques to ensure security of network. Apply authenticity to detect the malicious user and block them permanently. In this way, the network is prevented from damage.

Considering the importance of security in IoT applications, it is really important to implant security mechanism in IoT devices and communication networks. Moreover, to protect from any intruders or security threat, it is also recommended not to use default passwords for the devices and read the security requirements for the devices before using it for the first time. Disabling the features that are not used may decrease the chances of security attacks. Moreover, it is important to study different security protocols used in IoT devices and networks.

3.2 Privacy issues in IoT

The Internet of Things (IoT) can produce massive amounts of data. This data has to be transmitted, processed in some way, and then potentially stored somewhere, hopefully securely. (Pollmann, 2017) Much of this data is personal data, and some can be quite sensitive. This brings data privacy questions to the forefront.

The most dangerous part of IoT is that consumers are surrendering their privacy, bit by bit, without even realizing it [16], because they are unaware of what data is being collected and how it is being used. As mobile applications, wearables and other Wi-Fi-connected consumer products replace “dumb” devices on the market, consumers will not be able to buy products that don’t have the ability to track them. It is normal for consumers to upgrade their appliances, and it most likely does not occur to them that those new devices will also be monitoring them.

When considering data privacy regulations around the world, particularly those required by the EU’s General Data Protection Regulations (GDPR) [6] that go into effect in May of 2018, the amount of data generated by the growing IoT is an urgent concern. Both developers and users of IoT devices will be taken responsible for their use of personal data.

Privacy in the Internet of Things is the threefold guarantee to the subject for :

- Awareness of privacy risks imposed by smart things and services surrounding the data subject
- individual control over the collection and processing of personal information by the surrounding smart things

- awareness and control of subsequent use and dissemination of personal information by those entities to any entity outside the subject's personal control sphere

Table 3. The threefold of privacy in IoT

	Threats	solutions
Privacy in device	· Unauthorized access to IoT devices may result in sensitive information being leaked out.	· Location privacy of the device owner, protection of the personal information in case of the device theft or loss and resilience to side channel attacks should be provided.
Privacy in transit	· Sensitive information may be leaked out during the communication when plain text is transmitted without encryption.	· Encryption is a common tool to assure data confidentiality of data in transit. In case encryption adds data to packets which provides a way for tracing, pseudonyms could be replaced by identity information of IoT devices in order to decrease the vulnerability of the device's identity or user's being revealed.
Privacy at rest	· Unnecessary amount of personal information may be stored.	· Only necessary amount of information that is needed should be stored in the IoT device. · Only personal information should be retained, if unavoidable. · Information should be stored on the basis of the principle of "need-to-know".
Privacy at processing	· Personal information should be shared for the intended purpose of processing. · Personal information should not be disclosed to third parties, without explicit acceptance and the knowledge of the data owner.	· Encryption with appropriate access control, such as Digital Rights Management (DRM) [36] could be an appropriate tool which defends against illegal access to data. · User's permission and their awareness are required for disclosure, distribution of personal information. · De-identification techniques [37] could be used to conceal the real identity linked with the processed data.

Our definition of privacy captures in essence the idea of informational self-determination by enabling the subject to assess his personal privacy risks, to take appropriate action to protect his privacy, and to be assured that it is enforced beyond his immediate control sphere.

The data stewards, data architects, data administrators, and data modelers should review and use the following privacy requirements throughout the system development life cycle.

The following provides some privacy requirements to be considered [8]:

Purpose: Collect and process for purposes that are relevant to the services being provided. PI must not be collected or used for purposes that are materially different from the original purpose for which the data was provided.

Notice: System creators, owners, and fiduciaries must explain to users how their personal information will be used, collected, protected, retained, kept accurate, accessed, corrected, or otherwise processed before any processing occurs.

Choice/Consent: Data subjects must consent to the collection and use of their personal information.

Transfer: Data should not be transferred to third parties for their own use without the data subject's permission.

Access, Correction, Deletion: Data subjects must have a means of accessing the personal information that has been collected about them. They also are entitled to delete or amend false or inaccurate data.

Security: Use appropriate technical, logical, and administrative measures to ensure only authorized access and use of data.

Minimization: Collect and process the minimum necessary data to achieve the identified, legitimate intended purposes. The minimization principle is closely related to the purpose limitation requirement where only the necessary PI is collected and processed to achieve a legitimate purpose.

Proportionality: Data collection should be legitimately proportional to need, purpose, and sensitivity of data. This requirement can be one-step further abstracted to connect that data to quality and value.

Retention: Retain data only as long as it is required.

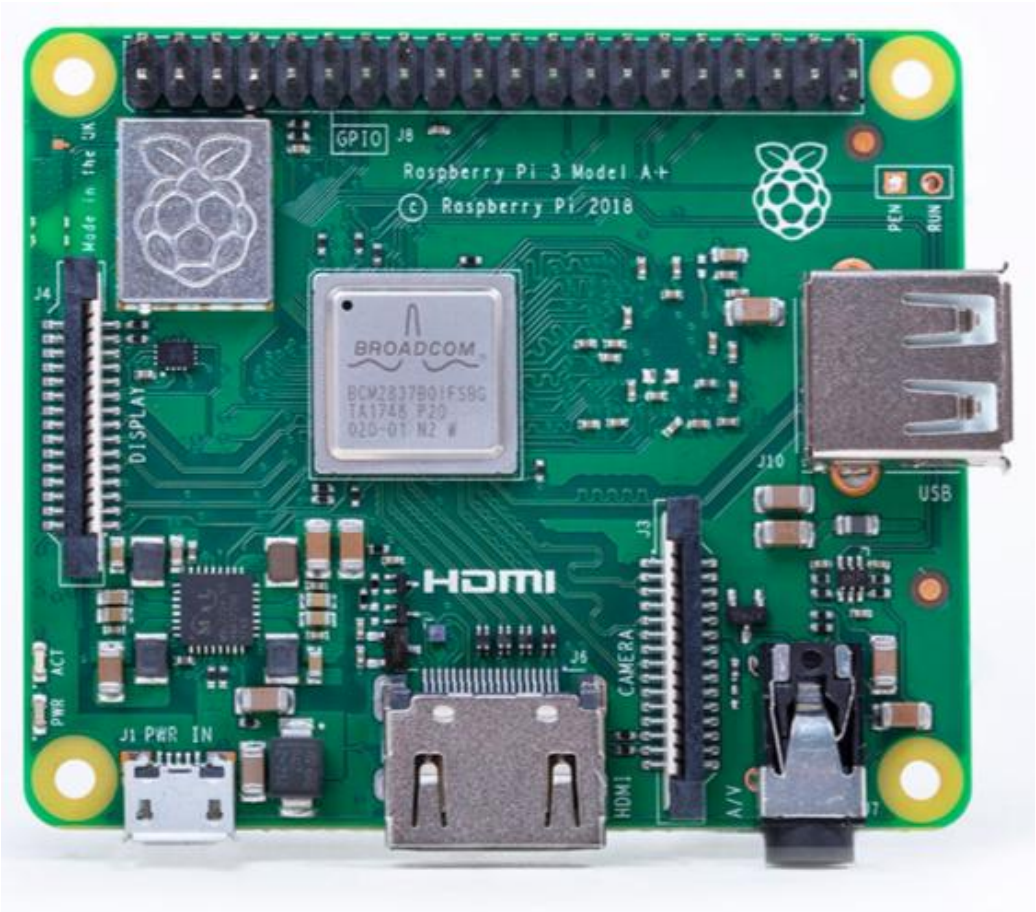
Act Responsibly: Put a privacy program in place.

4 CASE OF STUDY: LED LIGHT CONTROLLED VIA HTTP

For my LED controlled demonstration, I will use a very simple scheme, which anyone even with limited knowledge in electronics can reproduce, the idea is not how the complex the system is, but to show how ignoring basics security rules can lead to security or privacy leaks.

Here, we will talk and demonstrate at a very micro part of IoT system: Lightning; which can be used to save energy, or coupled to a motion detection for a security system, etc….

We won't reproduce the whole Home Automation system, with all the sensors and features.



To achieve this, I was decided to use a Raspberry Pi 3 model A+

Figure 7. Raspberry Pi 3 Model A+

Which got enough computing capabilities, here the official overview from the raspberry pi web site [13]:

The Raspberry Pi 3 Model A+ is the latest product in the Raspberry Pi 3 range. Like the Raspberry Pi 3 Model B+, it boasts a 64-bit quad core processor running at 1.4 GHz, dual-band 2.4 GHz and 5 GHz wireless LAN, and Bluetooth 4.2/BLE.

The dual-band wireless LAN comes with modular compliance certification, allowing the board to be designed into end products with significantly reduced wireless LAN compliance testing, improving both cost and time to market.

4.1 Electronic Parts

For our demonstration we will use a simple LED controlled via GPIO, we will need the following:

- A Raspberry Pi with Raspbian OS installed. I also recommend changing the default pi password.
- Access to a terminal on the Pi, either through a keyboard and screen, or Headless access to Pi through SSH.
- An LED.
- A 220 Ohm resistor.
- Some wires and a breadboard.

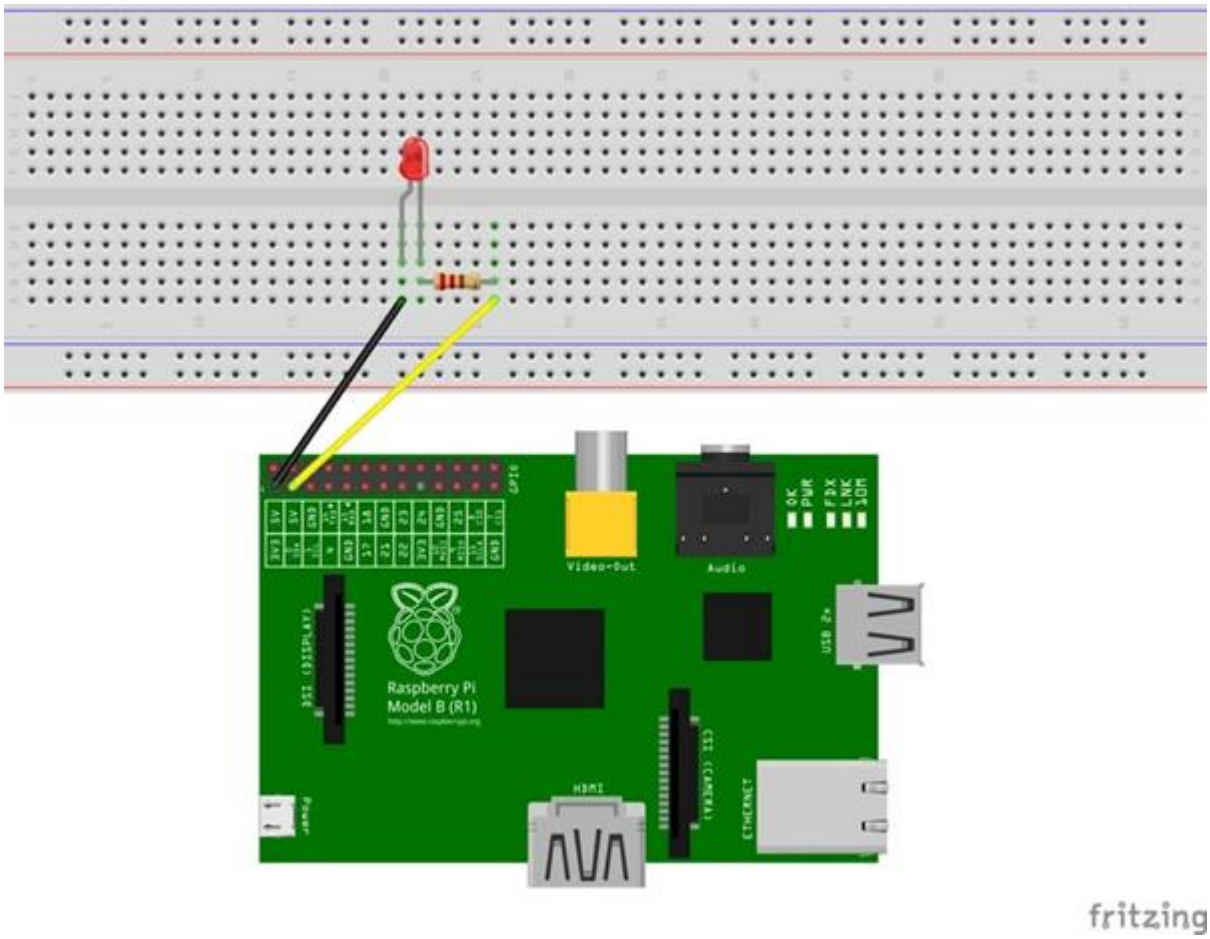


Figure 8. Scheme to control the LED

We connect our LED like following:

We connect the LED as shown in the picture. Connect the anode (longer pin) to the 3.3V pin on the Raspberry Pi. Connect one end of the 220 Ohm resistor to the cathode (short pin) and the other end to wiring pi pin 8 (SDA on all Raspberry Pi Model B boards).

4.2 Setting up our work environment

4.1.1 Raspberry pi

- The Pi: Raspberry Pi 3 Model A+
- microSD card 8gb
- microSD card reader
- Raspbian Os
- Power supply
- USB keyboard
- USB mouse

After downloading the Raspbian OS, we just need to flash our preformatted SD card, for that we used Balena Etcher:

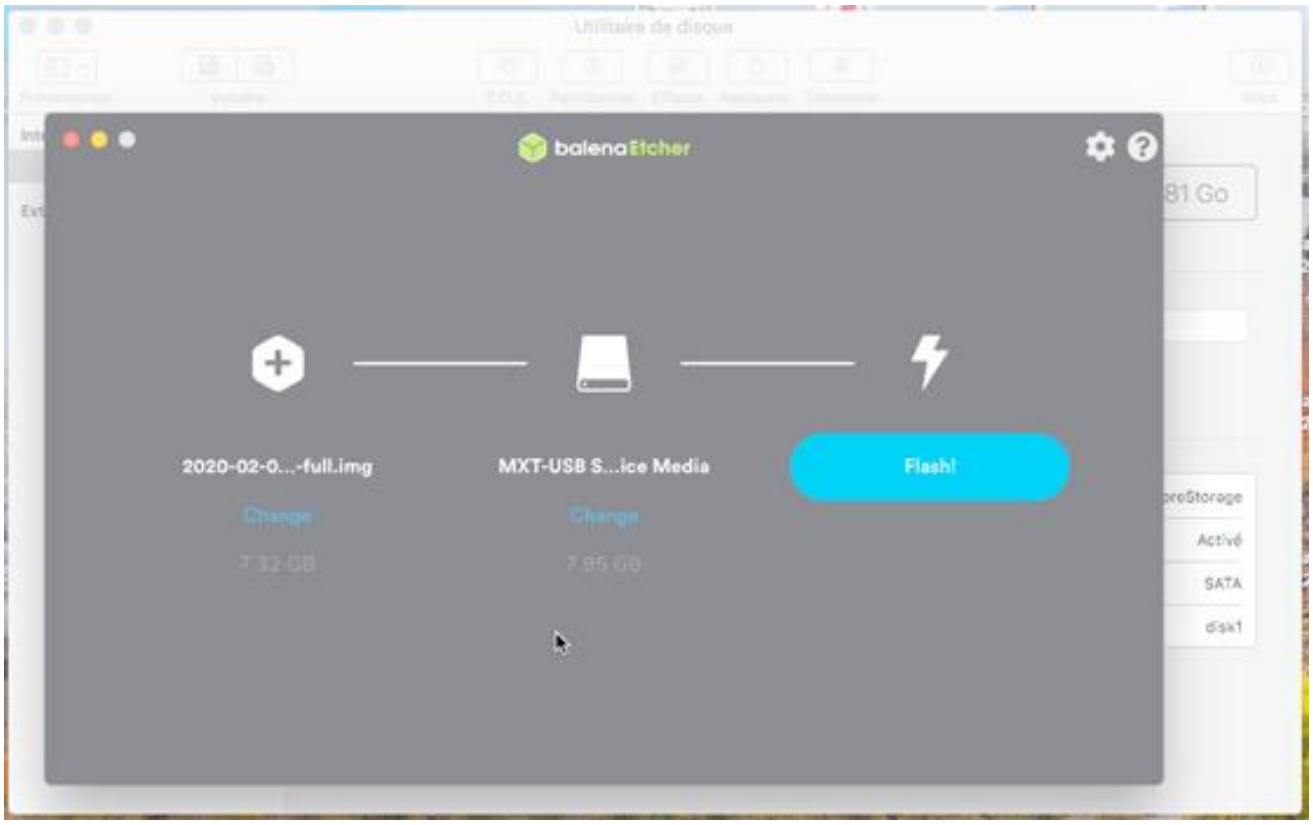


Figure 4.3. Flashing our SD card using Balena Etcher

After it completed, we just insert the **microSD card** with the fresh installed Raspbian into the card slot on the underside of the Raspberry Pi.

Once the operating system is installed on the SD card, take our board and turn it over.

The Raspberry Pi 3 A+ has a variety of ports on the front of the board. On the left, you've got a micro USB port for the power, in the middle, we've got a full-sized HDMI 1.3 port for hooking up TVs or monitors to the Raspberry Pi.

On the right hand edge of the board, we can also see the single USB 2.0 port. This is where we to connect mouse or keyboard to the Raspberry Pi, but there's always the option of adding more peripherals via Bluetooth.

Now that Pi is operational, we will enable SSH so we won’t be dependent to TV monitor. For security reasons, ssh is no longer enabled by default.

To enable it we need to place an empty file named ssh (with no extension) in the root of the boot disk [10] .

For mac users:

```
touch /Volumes/boot/ssh
```

Then we add network info create a file in the root of boot called: wpa_supplicant.conf

```
touch /Volumes/boot/wpa_supplicant.conf
```

See the figure [10] bellow :

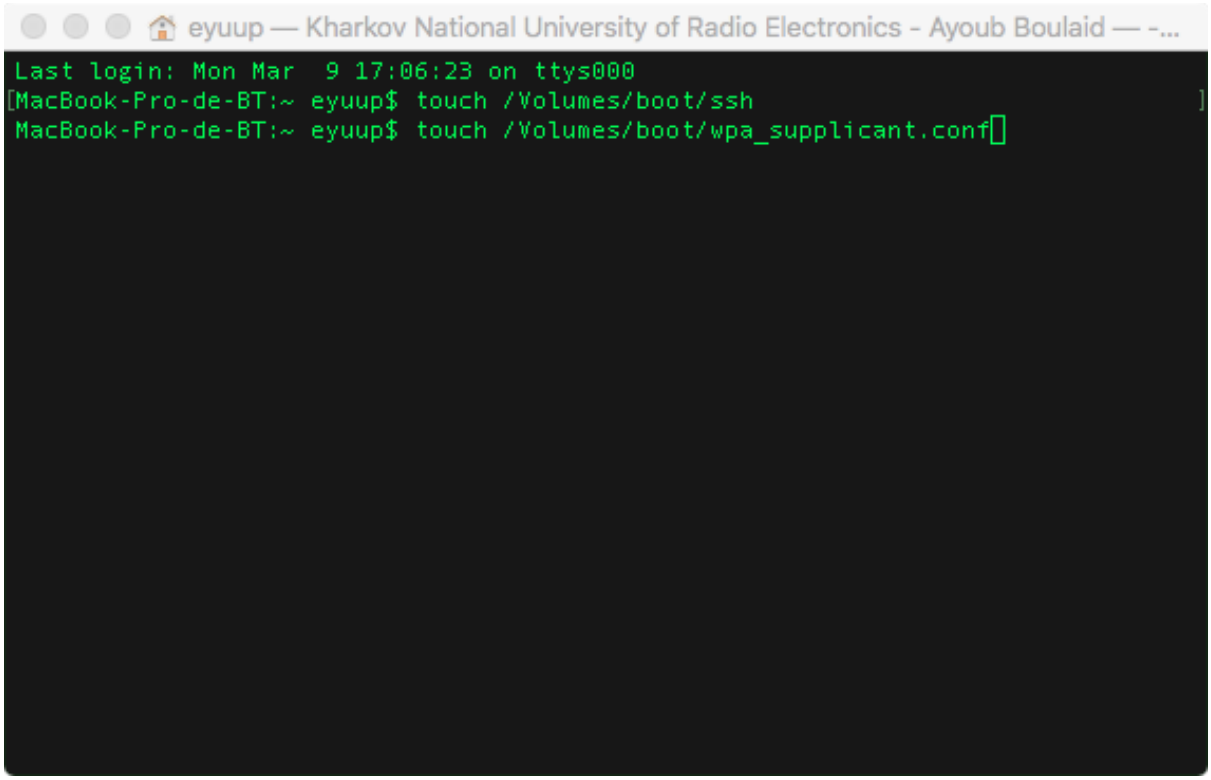


Figure 4.4. Creation of ssh and wpa_supplicant

Then using any text editor, we paste the following into it (see Appendix A) :

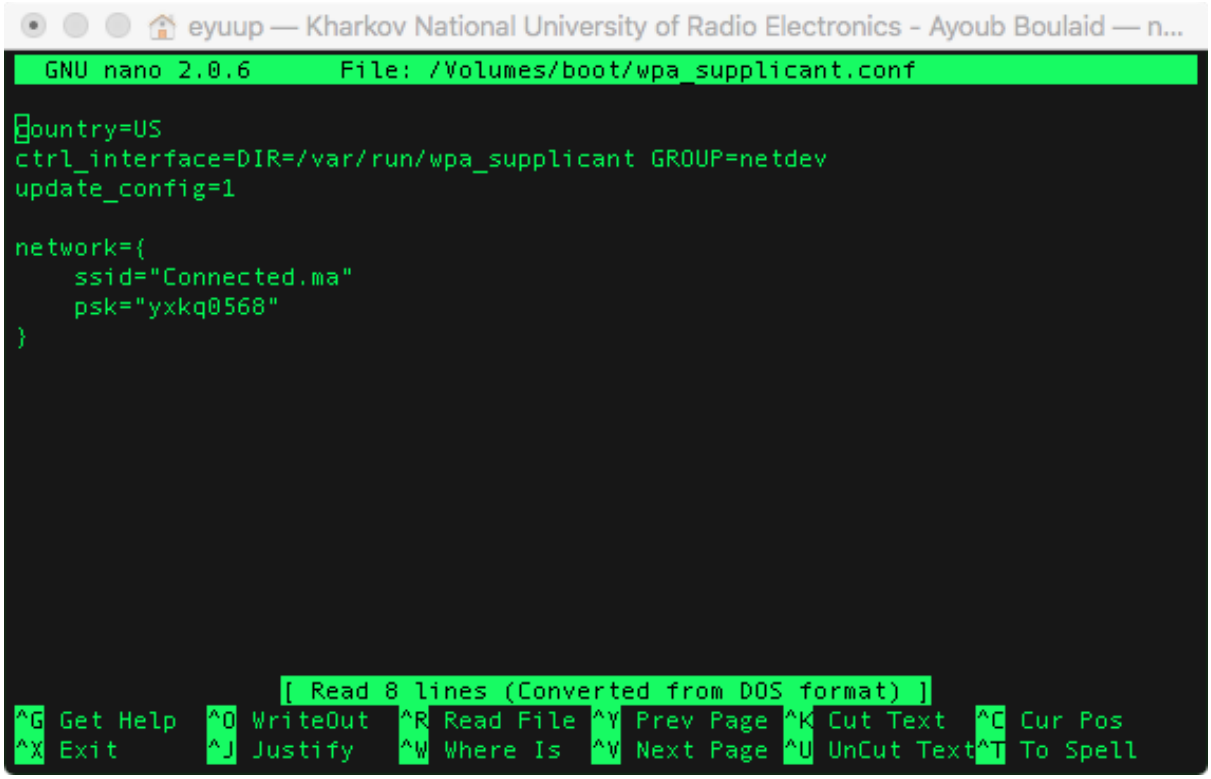


Figure 4.5 Wi-fi Network configuration

For Windows users we can use Notepad to edit our wpa_supplicant.conf file (wifi settings)

- Run **Notepad**
- Paste in the contents above
- Click **File / Save As …**
-

Be sure that ***wpa_supplicant.conf*** got .conf extension not .conf.txt and save it

Now, that everything is setup, let's boot and connect to our Pi, we open new terminal and type:

The default user name is: **pi**

The default password is: **raspberry**

Because your pi is now on the network, you should immediately change the hostname and password.

To get the Pi IP address, we could from our computer, which should be in the same network as the PI, using the ping command [4.6]

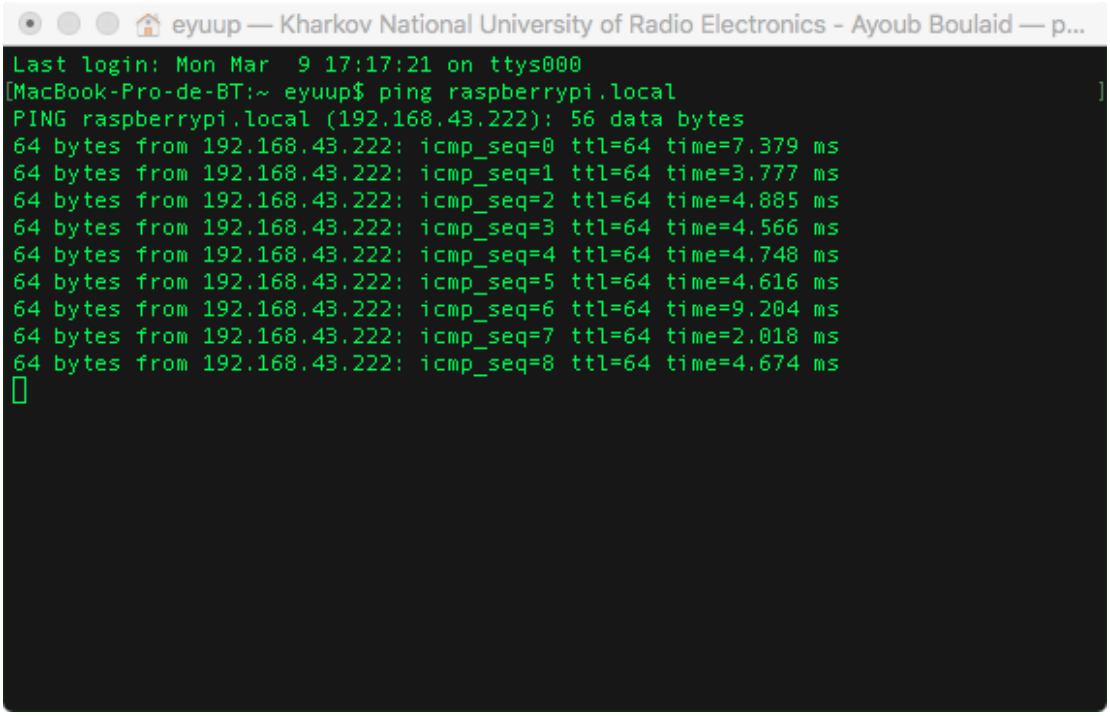


Figure 12. Ping to the PI

For that, in our computer terminal we type:

```
ping raspberrypi.local
```

Now that Pi is on and is connected to our network, let’s do so configuration routine starting by changing our default password as we said before.

Let’s start by connecting to it:

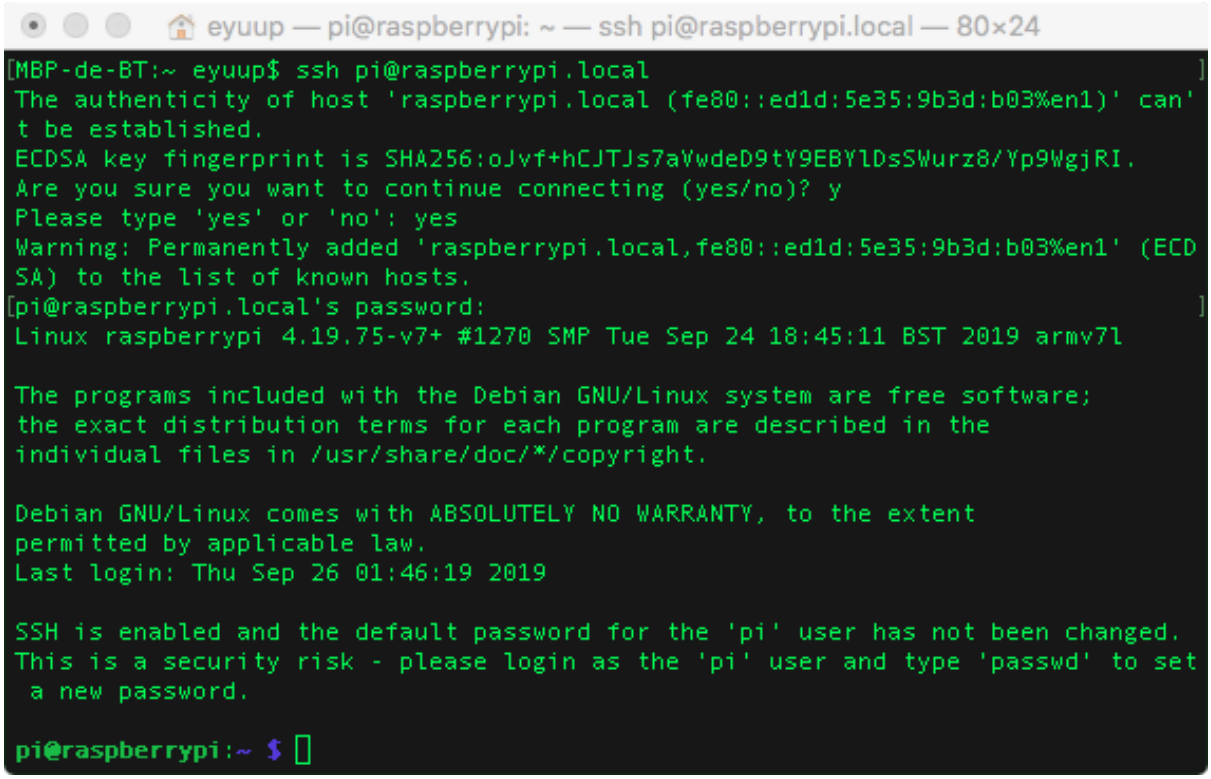


Figure 4.7 Connecting remotely to Pi via SSH

For that, in our computer terminal we type:

```
sh-keygen -R raspberrypi.local

ssh pi@raspberrypi.local
```

Now we could start the tool to configure the Pi and select the options for changing the hostname and password and much more.

```
sudo raspi-config
```

Once the changes are done, just reboot.

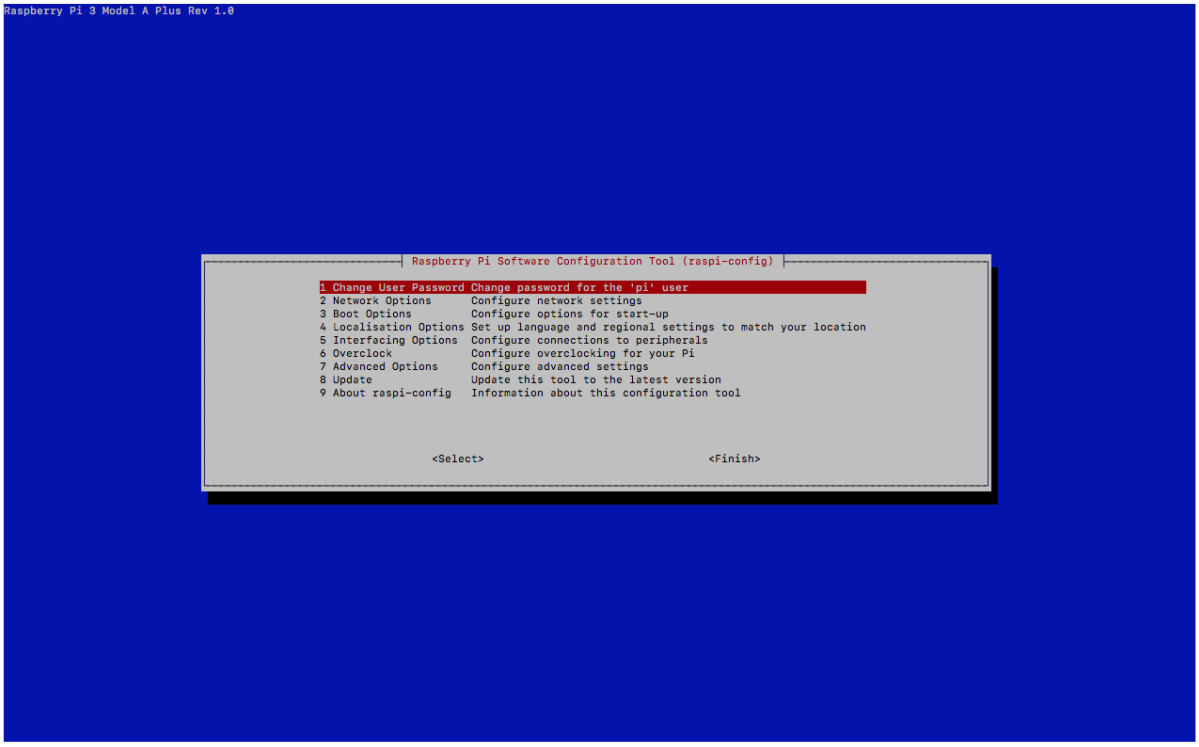


Figure 4.8 Raspian Configuration tool

After we reboot our Pi, it's highly recommended to get Updates:

```
sudo apt-get update -y

sudo apt-get upgrade -y
```

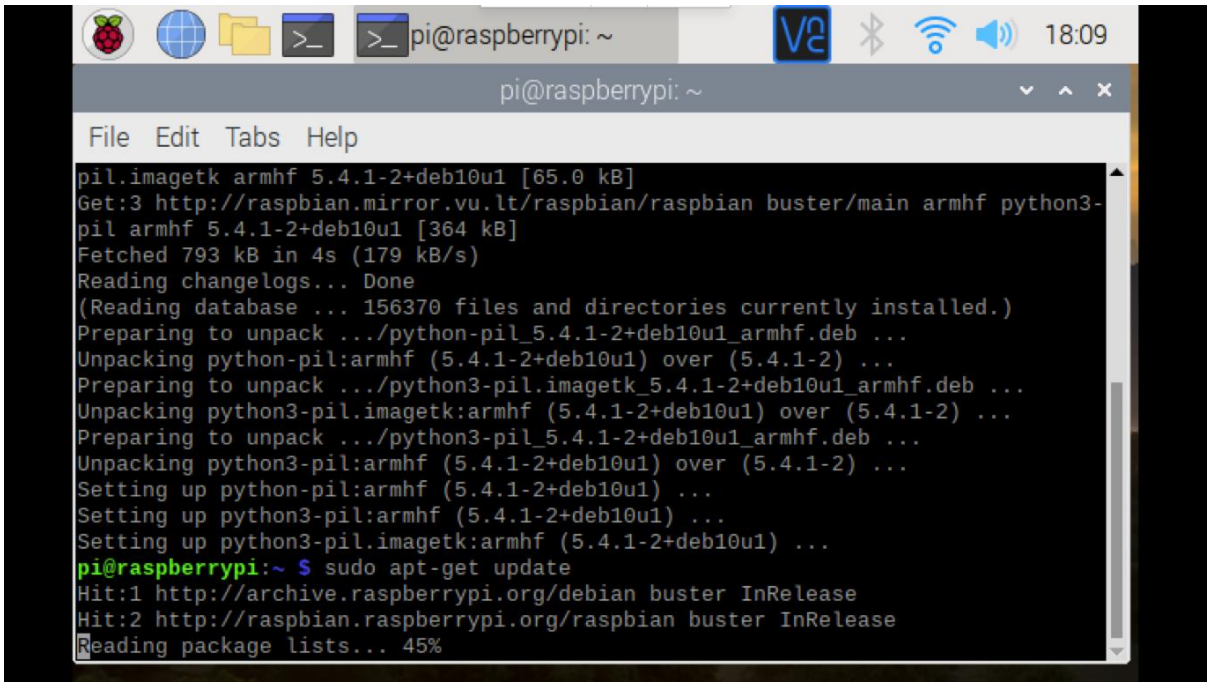


Figure 4.9. Getting Updates/Upgrades of packages

Next, we should install WiringPi [15] which is a PIN based GPIO library written in C for the BCM2835, BCM2836 and BCM2837 SoC devices, that is used in all Raspberry Pi boards. It is under the GNU LGPLv3 license and is usable from C, C++ and RTB (BASIC) as well as many other languages with suitable wrappers.

For that, we use the git method:

```
git clone https://github.com/WiringPi/wiringPi.git
```

Then install it using:

```
cd WiringPi ./build
```

After getting thing done, we now installing apache Server, which is a very popular webserver, designed to create web servers that have the ability to host one or more HTTP-based websites. Apache can be enhanced by manipulating the code base or adding multiple extensions/add-ons. In our project we are using an HTTP server and its PHP extension.

To Install Apache web server we will use following commands in our terminal to install the apache2 package:

```
sudo apt-get install apache2 -y
```

To test the web server whether it is working or not, we open our browser and type the Pi’s IP address in the tab.

To find the Pi's IP address, there is different method we just use *ifconfig* at the command line.

By default, Apache [14] puts a test HTML file in the web folder. This default web page is served when you browse to http://192.168.1.107 (or whatever the Pi's IP address is) from another device on the same network, we should see the following in Figure [15], which means that Apache web server is working fine.

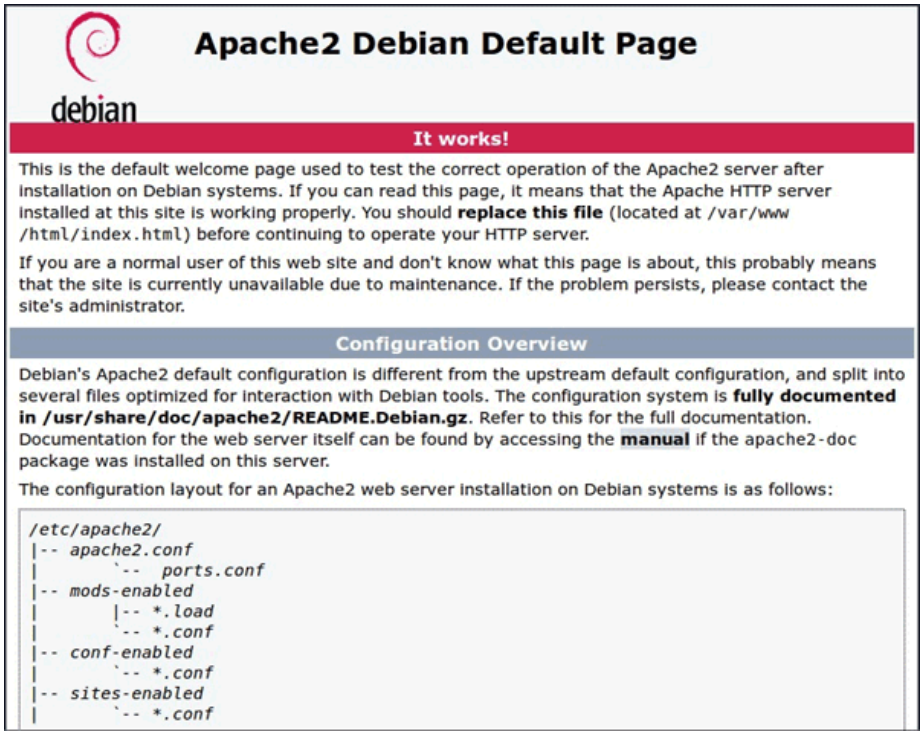


Figure 4.10. Apache default page

4.1.2 Testing code

Before we discuss http server, let's just read Raspberry Pi's GPU temperature, and also try to control the LED. Just like in programming let's experience our first hello world with Raspberry Pi.

Reading GPU temperature is used to demonstrate of getting some data from Raspberry Pi, It was decided to read the GPU temperature because it is unique to Raspberry Pi.

We could just type in a bash shell command the following to get the GPU's temperature:

```
/opt/vc/bin/vcgencmd measure_temp
```

Which returns the following results:

```
temp=41.5'C
```

And using these commands to control the LED

```
/usr/local/bin/gpio -g write 17 0

/usr/local/bin/gpio -g write 17 1
```

Now, that’s everything seems to work, we just need to change our permissions to make our landing page that will control our LED.

This default web page is just an HTML file on the file system. It is located at ***var/www/html/index.html***.

We go to this directory in a terminal window and have a look at what's inside:

```
cd  var/www/html
ls -al
This will show you:
total 12
drwxr-xr-x  2 root root 4096 Feb 27 01:29 .
drwxr-xr-x 12 root root 4096 Feb 27 01:28 ..
-rw-r--r--  1 root root  177 Feb 27 01:29 index.html
```

This shows that by default there is one file in */var/www/html/* called ***index.html*** and it is owned by the root user . To edit the file, you need to change its ownership to your own username. Change the owner of the file using:

```
sudo chown pi: index.html
```

We can now start editing this file and start writing the code for our landing page or web application.

4.1.3 Web interface

Now that we have apache installed and working fine, permissions accorded to our user and we can edit file, before we go further with our project, we decided to use PHP for controlling GPIO and our LED, for that we want to use PHP code along with HTML so we have to install the PHP extension in Raspberry pi.

Using PHP code allows us to use shell commands to control the LED from PHP script. To allow Apache server to edit PHP files, we will install the latest version of PHP and the PHP module for Apache. Use the following command in terminal to install these:

```
sudo apt-get install php libapache2-mod-php -y
```

Now we remove the default index.html file:

```
sudo rm index.html
```

And create our own index.php file:

```
sudo nano index.php
```

Now we enter the below code in *index.php* to test the PHP installation.

```
<?php phpinfo(); ?>
```

We save it by pressing CTRL + X (or CMD+X for mac users) and the ‘y’ and enter. Now refresh the webpage in our browser and we should see a long page with lots of information about PHP. This shows that the PHP extension is installed properly.

We open our Pi’s address in our browser and we should get php info’s as shown in figure [17]

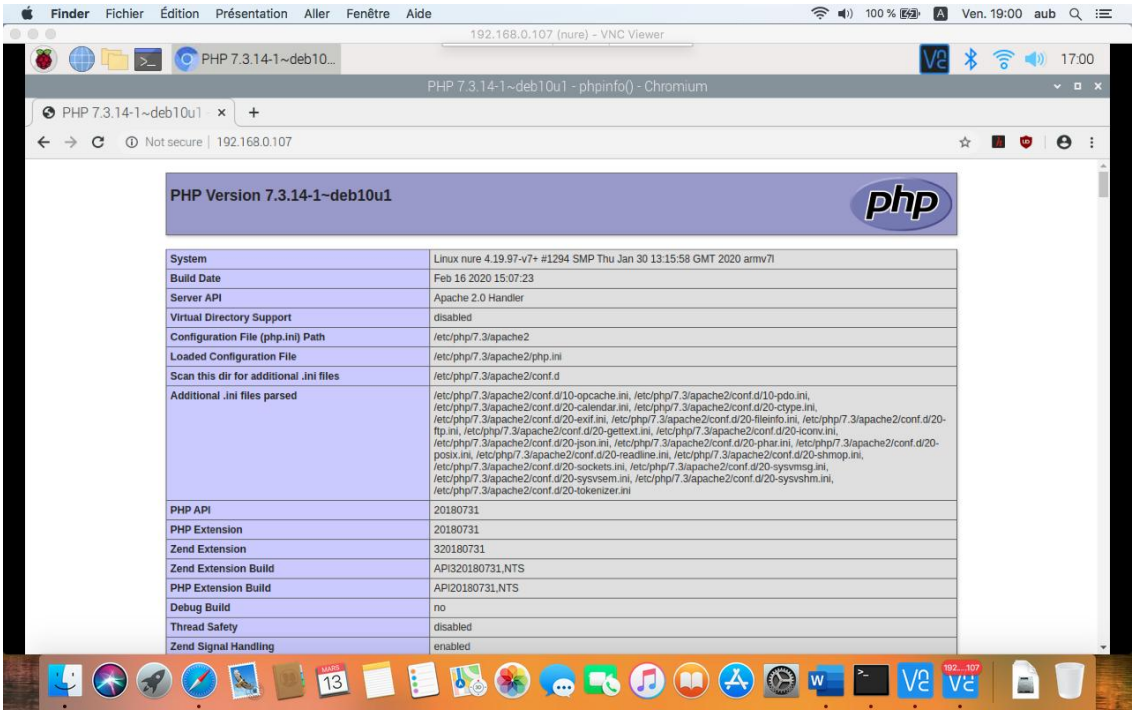


Figure 4.11. PHP info displayed in our browser

Now we up to start writing the code to control GPIO pins, so we delete the previous code in *index.php* (<?php phpinfo(); ?>) file and insert below our PHP code to control GPIO pins inside body of HTML code see Appendix B.

```
<html>

<head>

<meta name="viewport" content="width=device-width" />

<title>Raspberry Pi WiFi Controlled LED</title>

</head>

<body><center><h1>Control LED using Raspberry Pi Webserver</h1>      <form method="get" action="index.php">

<input type="submit" style = "font-size: 14 pt" value="OFF" name="off">

<input type="submit" style = "font-size: 14 pt" value="ON" name="on">

</form></center>

<?php
```

```
shell_exec("/usr/local/bin/gpio -g mode 17 out");
            if(isset($_GET['off']))
            {
         echo "LED is off";
shell_exec("/usr/local/bin/gpio -g write 17 0");     }
else if(isset($_GET['on']))
{
            echo "LED is on";
shell_exec("/usr/local/bin/gpio -g write 17 1");
}
?>
</body>
</html>
```

Here we have used ***shell_exec()*** command in php code, this command is used to run the shell command from the PHP script. If you run the command inside *shell_exec* directly form the terminal of Raspberry pi, you can directly make GPIO pin 17 low or high. Below are two commands to test the LED directly from terminal.

```
/usr/local/bin/gpio -g write 17 0
/usr/local/bin/gpio -g write 17 1
```

4.1.4 Testing our system:

After completing this, we could access our PHP page in our browser by typing the IP address of raspberry pi in the browser. With the 2 buttons - ON, OFF we control our GPIO pins, for our study the LED.

Figure 4.12 Our landing page

4.3 Penetration test

In this section, we will discuss how we can bypass security level considering how we built our system.

As every penetration test, we start by gathering information about our victim devices / network, in that line, we already now that the LED is controlled via Wi-Fi, commanded by a web page with two buttons ON/OFF.

In this spirit, let's consider that we already in or hacked the Wi-Fi network, now we need to know the IP address of the Pi, for that we can use ARP Scan tool (also called ARP Sweep or MAC Scanner) which is a very fast ARP packet scanner that shows every active IPv4 device on the Subnet.

The ARP Scan Tool is very useful to find hidden devices even if they have firewalls. Because devices cannot hide from ARP packets like they can hide from Ping ones.

ARP Scan tool [19] is very simple, so for our case, we will list active devices in our Subnet Figure [19], using this command in out terminal:

```
sudo arp-scan –l
```

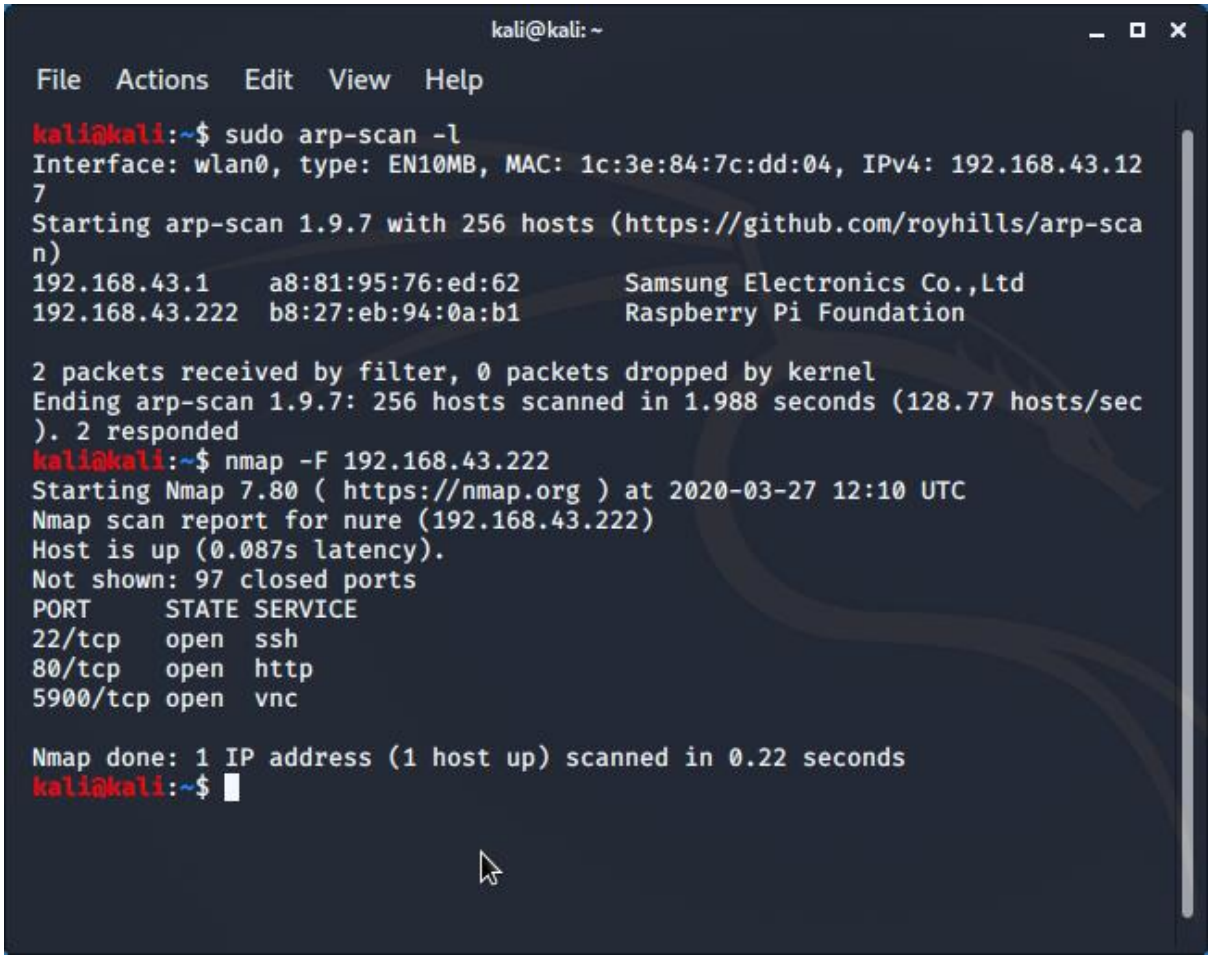


Figure 19. Results of arp-scan listing active devices, and fast scan using nmap

Arp-scan tool returned the ip address active devices in the network where our targeted PI is connected, now let's gather some information so we choose which way we will try to penetrate our system.

Using the very popular Nmap tool [18], we start with a fast scan to see which ports and which services are running in our target, in the previous figure [19], we can see that our target is running a ssh, a web and VNC server.

At this point let's check what's running on port 80, for that we just open our browser and point the http://192.168.43.222

As previously in figure 18, we got in the landing page, and we control the LED.

At this stage of how our system was built, the security is very critical, in other words, there’s no security level at this stage and anyone in our network could easily control GPIO, to rectify that, let's modify the landing page of our server and add credential.

Let's add a login page to limit access to the pi's page that control our GPIO.

We have displayed one text field for login, one Password field, Reset button and Login button. We have used Reset button that resets all fields to blank. We have used JavaScript validation in Login page. We have set username and password value.

Login page is used in most of the dynamic website to validate user based on their credentials. For making login page for websites HTML forms and HTML elements are used. Text field is used to enter username and password text field is used to type password from user.

The submit button is used for submitting data to server for validation. It’s good to validate user input in the browser using JavaScript. We decided to make client-side to show how easily it can be bypassed.

If credentials are correct, then we are redirected to the page with our LED control, if not then we got an error.

Here the code for our freshly created page see appendix C:

```
<html>

<head>

<title>Login Page</title>

</head>

<body>

<form name="loginForm" method="post" action="login.php">
```

```
<table width="20%" bgcolor="0099CC" align="center">
<tr>
<td colspan=2><center><font size=4><b>HTML Login Page</b></font></center></td>
</tr>
<tr>
<td>Username:</td>
<td><input type="text" size=25 name="userid"></td>
</tr>
<tr>
<td>Password:</td>
<td><input type="Password" size=25 name="pwd"></td>
</tr>
<tr>
<td ><input type="Reset"></td>
<td><input type="submit" onclick="return check(this.form)" value="Login"></td>
</tr>
</table>
</form>
<script language="javascript">
function check(form)
{
if(form.userid.value == "nure" && form.pwd.value == "password")
{
      return true;
```

```
}
else
{
      alert("Error Password or Username")
      return false;
}
}
</script>
</body>
</html>
```

Now our landing page go through authentication, then the landing page, Appendix [1],[2] we can see both code source of the login page and the updated landing page:

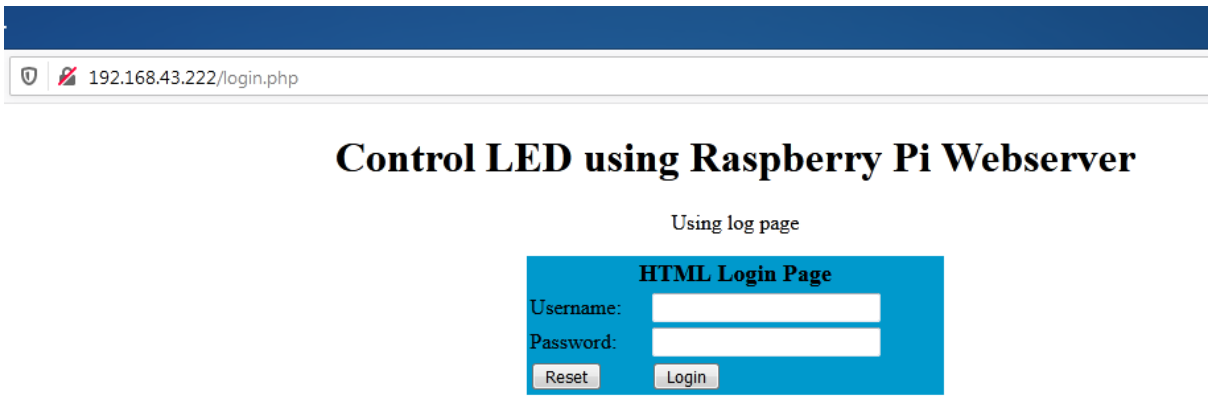


Figure 4.14. Login page

If the login and password matched we will got access granted, if not then a JavaScript alert pops in with the error message as we can see in both Figures [4.14] and [4.15].

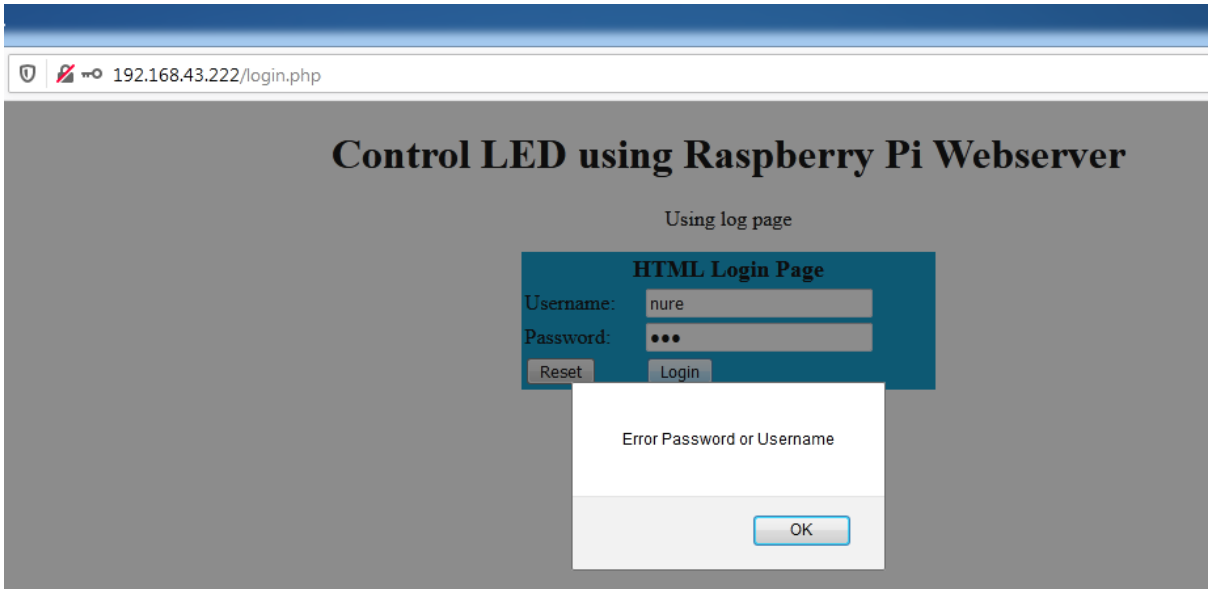


Figure 21. Password or login not valid.

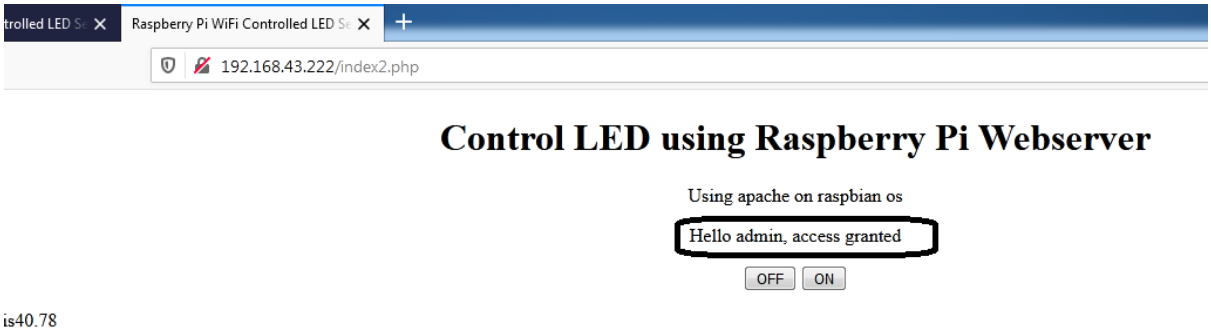


Figure 4.16. Access granted

As we see, now to get to the landing page, we should get both login and password, at that stage many methods could let us by pass this system.

As in the figure [4.15], we could see a JavaScript alert, that could let us think that the login and password are saved in the script itself, or we could perform a man-in-the-middle attack and sniff the network hoping that the user will type the credentials.

In this spirit let’s start by check the code source, a simple look to it, and we can easily understand that's our credential are saved in plain text, which is critical for our system, we don't even need to use tools like Wireshark to sniff/capture the traffic and get the login and password in plain text. Figure [4.17]

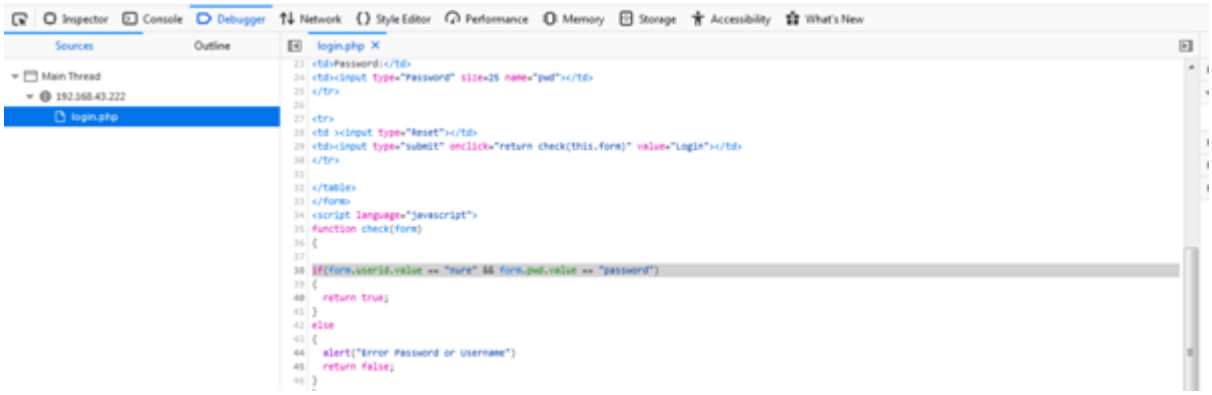


Figure 4.17. Code source of the login page

Here we clearly can see the login : nure, and the password : password as plain text.

```
if(form.userid.value == "nure" && form.pwd.value == "password")
```

Even worst of that, with little bit of HTML, JavaScript knowledge, we deduct that the form of the login page sending the value of login field, and password one to index2.php if the login password matched what we code in our script, and if we go directly and point our browser the this last, we just get it without even typing credentials, which lead us to the landing page, with the mention access granted, which means almost no security levels.

To fix that we propose to go for a server side authentication system, and to encrypt data that we pass via POST or GET methods, using authentication systems stored in server side, not client side, so even if an attacker could

intercept the traffic, at least it won't be a simple look at the source code to found out our credentials at human readable form.

So for better security, we should go for a server-side authentication, because client-side is extremely weak and may be bypassed easily. Any attacker may read the source code and reverse-engineer the authentication mechanism to access parts of the application which would otherwise be protected.

We also recommend to use HTTPS instead of HTTP protocols [10], with TLS encryption, using PHP, we should not ignore attacks like XSS which goes for Cross site scripting, SQL injection, for example with the help of function like html_entities in php to process and pass data and limit XSS attacks.

We could increase security level by using encryption technique so that attacker will not able to use user credentials. But here again, an attacker could use Fiddler tool for packet capturing and have the capability of replaying the captured packet.

Assuming that, in my opinion, the final patch to fix this issue is to use access token along with encrypted user credentials so the attacker will not able to do any type of attack involving, packet capturing or packet replaying, because replay packet token will not match and will get refused.

It is also crucial to secure our web server, keep in it updated, check permissions, using .htaccess

However, in reality, we must plan at least some of your security strategy our self by using security rules.

I compiled the following best practices to help protect our IoT ecosystem for further progression and continuous, from design and implementation to further operations and management. These recommendations are not an exhaustive list and only clarify the underlying concepts behind each rule.

- Every device and systems should have unique identities and credentials.

- We set authentication and access control mechanisms.
- Using cryptographic network protocols.
- Create continuous update and deployment mechanisms.
- Deploying security auditing and monitoring mechanisms.
- Continuously be updated of new vulnerabilities for our implemented security mechanisms.
- Avoid unnecessary data access, storage, and transmission

4.4 Analyzes of results

As we said before, we considered that we have access to Wi-Fi or hacked it, the router is considered the “front door” to your smart home or to any system or network depending on it. Like any front door, it should be solid and equipped with strong locks, in case cyber criminals come knocking.

Building a more secure IoT system starts with Wi-Fi router. It’s the main and essential devices that connects all your connected devices and let them operational to do tasks they are supposing to do.

Most people simply use the router provided by their internet service provider, or buy themselves some other router of any company in the market, but a majority of people don't change default password, use some predictable and simple key for their Wi-Fi key, or let some features enabled that they don't use but hackers can be happy to found on your devices.

For example Universal Plug and Play (UpnP), which is a set of networking protocols that permit networked devices, such as computers, printers, Wi-Fi access points and mobile devices to seamlessly discover each other on the network and establish functional network services for data sharing, communications, and entertainment. Which could be used by ill-intentioned person to use a device in the target network to gain access to many other

devices and perform attacks like on smart TV, printers, baby monitoring cameras.

Then came to secure your IoT devices, they might come with default privacy and security settings. It’s become a must to changing them, as some default settings could benefit the manufacturer more than they benefit you.

IoT devices come with a variety of services such as remote access, often enabled by default. If you don’t need it, be sure to disable it.

Depending of manufacturer, you should periodically update your software, and even your firmware, and some time even upgrade your hardware to get part of fixes, patches and security update.

As our demonstration, we could first check the configuration of our apache, limit information breach, and check permissions.

As it's hard to control every aspect of our system due to the variety of technologies, but at least we must do the effort to pay attention to simple security breaches due to misconfiguration or bad choice of system chosen.

The main problem is that because the idea of networking appliances and other objects is relatively new, security has not always been considered by manufacturers in designing their products.They use old firmwares with unpatched software. In the other side, users forgot or ignor changing the default passwords on smart devices or if they do change them, they use very weak passwords.

To improve security, an IoT device that needs to be directly accessible over the Internet, should be segmented into its own network and have network access restricted. The network segment should be monitored to identify potential threats.

CONCLUSION

The Internet of Things promises to deliver a step change in individual's quality of life and enterprise's productivity. Through a widely distributed, locally intelligent network of smart devices, the IoT has the potential to enable extensions and enhancements to fundamental services in transportation, logistics, security, utilities, education, healthcare and other areas, while providing a new ecosystem for application development.

A concerted effort is required to move the industry beyond the early stages of market development towards maturity, driven by common understanding of the distinct nature of the opportunity. This market has distinct characteristics in the areas of service distribution, business and charging models, capabilities required to deliver IoT services, and the differing demands these services will place on mobile networks.

International standardization developing groups are striving to develop standards to address security and privacy issues for IoT. IoT has entered a phase of mass usage and it could not acceptable that 70% of IoT devices have major security vulnerabilities. It would take some time for IoT security standards to reach at a level where customers can feel confident in the security of a device based on a security rating, but it is believed that it is time to start this work to meet urgent market needs. As security may be an enabling factor of many of major IoT applications, detailed security mechanisms and protocols including organizational management issues to secure communications are fundamental.

Conventional security primitives cannot be applied due to the heterogeneous nature of sensors, low resources and the system architecture in IoT applications. To prevent unauthorized use of user's data, protect their privacy and to mitigate security and privacy threats, strong network security infrastructures are required. Peer authentication and End-to-End data protection are crucial requirements to prevent eavesdropping on sensitive data or malicious

triggering of harmful actuating tasks. Any unauthorized use of data may restrict users to utilize IoT based applications. This review paper provides the security solution approaches been proposed recently identifying both the challenges related to security and privacy and the attack techniques used to compromise/fail the sensor nodes in Internet of Things as well. Current approaches are focused on pre- deployed, pre-shared keys on both ends whereas certificate-based authentication is generally considered infeasible for constrained resource sensors. New security paradigm is needed for End-to-End secure key establishment protocols that are lightweight for resource-constrained sensors and secure through strong encryption and authentication.

Even with the guidance available, there remain challenges around the design, implementation, and management of the IoT. In this paper we have discussed some of these challenges, from definition of the IoT, to specific challenges such as eliciting and managing consent. It is clear that significant progress is being made, but there is still a long way to go in the battle to secure the IoT.

LIST OF REFERENCES

1. Systems and Information Engineering Design Symposium (SIEDS). Proceedings of a meeting [Електронний ресурс]. – 27 April 2018. – 292 (1 Vol). – 300 p. Режим доступу: https://ieeexplore.ieee.org/xpl/conhome/8370613/proceeding

2. Alhalafi N., Veeraraghavan P. Privacy and Security Challenges and Solutions in IOT: A review 2019 IOP Conf. Ser.: Earth Environ. Sci. 322 012013 IOP Conference Series: Earth and Environmental Science. [Електронний ресурс]. – 2019. – 5 p. Режим доступу: https://iopscience.iop.org/article/10.1088/1755-1315/322/1/012013

3. Meola A. A look at examples of IoT devices and their business applications in 2020. Business Insider Intelligence [Електронний ресурс]. – Режим доступу: https://www.businessinsider.com/internet-of-things-devices-examples

4. IoT Tutorials. IoT Security – Major Problems Faced by IoT System. Data-flair training [Електронний ресурс]. – Режим доступу: https://data-flair.training/blogs/iot-security/

5. Muhammad A. Iqbal, Oladiran G. Olaeye, Magdi A. Bayoumi. A Review on Internet of Things (Iot): Security and Privacy Requirements and the Solution Approaches. Global Journal of Computer Science and Technology: E-Network, Web& Security. [Електронний ресурс]. – Vol. 16, Iss. 7, V.1.0. – 2016. – 9 p. – Режим доступу: https://globaljournals.org/GJCST_Volume16/1-A-Review-on-Internet-of-Things.pdf

6. Solving the IoT privacy problem. [Електронний ресурс]. – Режим доступу: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/broader-perspectives/solving-iot-privacy-problem.html

7. Finneran T. Privacy and Internet of Things (IoT). The Data Administration Newsletter. [Електронний ресурс]. – 2017 – Режим доступу: https://tdan.com/privacy-and-internet-of-things-iot/17539#_ftnref5

8. BalenaEtcher - a tool to burn the image to the micro SD card for you [Електронний ресурс]. – Режим доступу: https://www.balena.io/etcher/

9. HEADLESS RASPBERRY PI 3 B+ SSH WIFI SETUP (MAC + WINDOWS). [Електронний ресурс]. – Режим доступу: https://desertbot.io/blog/headless-raspberry-pi-3-bplus-ssh-wifi-setup

10. Gunawan T., Yaldi I., Kartiwi M., Ismail N., Zabah N., Mansor H., Nordin A. Prototype Design of Smart Home System using Internet of Things. Indonesian Journal of Electrical Engineering and Computer Science. – 2017. – pp.107-115. [Електронний ресурс]. – Режим доступу: 10.11591/ijeecs.v7.i1.pp107-115.

11. Mirza Abdur Razzaq, Sajid Habib Gill, Muhammad Ali Qureshi, Saleem Ullah. Security Issues in the Internet of Things (IoT): A Comprehensive Study. International Journal of Advanced Computer Science and Applications(IJACSA). – Vol. 8, No. 6. – 2017. – [Електронний ресурс]. – Режим доступу: http://dx.doi.org/10.14569/IJACSA.2017.080650

12. Forest C.Ten examples of IoT and Big Data working well together. Part of a ZDNet Special Feature: The Power of IoT and Big Data. – 2015.– [Електронний ресурс]. – Режим доступу: *https://www.zdnet.com/article/ten-examples-of-iot-and-big-data-working-well-together/*

13. Raspberry Pi Official [Електронний ресурс]. – Режим доступу: https://www.raspberrypi.org/products/raspberry-pi-3-model-a-plus/

14. Apache official [Електронний ресурс]. – Режим доступу: http://httpd.apache.org/

15. WiringPi [Електронний ресурс]. – Режим доступу: http://wiringpi.com/

16. Ziegeldorf, J. H., Garcia Morchon, O., Wehrle, K. Privacy in the Internet of Things: Threats and Challenges. Security and Communication Networks. – Vol. 7.12. – 2015. – 14 p.

17. Cyber Security Centre, WMG, University of Warwick, Coventry, UK Maple, Carsten. (2017). Security and privacy in the internet of things. Journal of Cyber Policy. – Vol. 2. – pp. 155-184 [Електронний ресурс]. – Режим доступу: 10.1080/23738871.2017.1366536.

18. Nmap Security Scanner. Port Scanning Techniques : Chapter 15. Nmap Reference Guide [Електронний ресурс]. – Режим доступу: https://nmap.org/book/man-port-scanning-techniques.html

19. ARP scanner [Електронний ресурс]. – Режим доступу: https://www.netscantools.com/nstpro_arp_scan.html

ВІДОМІСТЬ ВИКОНАННЯ АТЕСТАЦІЙНОЇ РОБОТИ

	Прізвище та ініціали відповідальної особи	Підпис	Дата
Роботу виконав: студент групи АМСЗІм-18-2	Булаід Айюб		
Керівник роботи:	Радівілова Т.А.		
Нормоконтроль проведено:	Снігуров А.В.		
Перевірка на плагіат здійснена. Рівень оригінальності тексту пояснювальної записки атестаційної роботи складає _____ %	Волотка В.С.		

Appendix

Appendix A : wpa_supplicant.conf

```
  country=US
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev
update_config=1

network={
    ssid="612"
    psk="omar6127"
}
```

Appendix B : index.php

```
<html>
<head>
<meta name="viewport" content="width=device-width" />
<title>Raspberry Pi WiFi Controlled LED</title>
</head>
<body><center><h1>Control LED using Raspberry Pi Webserver</h1>      <form
method="get" action="index.php">
<input type="submit" style = "font-size: 14 pt" value="OFF" name="off">
<input type="submit" style = "font-size: 14 pt" value="ON" name="on">
</form></center>
<?php

shell_exec("/usr/local/bin/gpio -g mode 17 out");

            if(isset($_GET['off']))

            {

         echo "LED is off";

shell_exec("/usr/local/bin/gpio -g write 17 0");      }

else if(isset($_GET['on']))

{

            echo "LED is on";

shell_exec("/usr/local/bin/gpio -g write 17 1");

}

?>

</body></html>
```

Appendix C: login.php

```
<html>
<head>
<title>Login Page</title>
</head>
<body>
<form name="loginForm" method="post" action="login.php">
<table width="20%" bgcolor="0099CC" align="center">

<tr>
<td colspan=2><center><font size=4><b>HTML Login Page</b></font></center></td>
</tr>
<tr>
<td>Username:</td>
<td><input type="text" size=25 name="userid"></td>
</tr>
<tr>
<td>Password:</td>
<td><input type="Password" size=25 name="pwd"></td>
</tr>

<tr>
<td ><input type="Reset"></td>
<td><input type="submit" onclick="return check(this.form)" value="Login"></td>
</tr>

</table>
</form>
<script language="javascript">
function check(form)
{

if(form.userid.value == "nure" && form.pwd.value == "password")
{
	return true;
}
else
{
	alert("Error Password or Username")
	return false;
}
}
</script>
</body>
</html>
```