

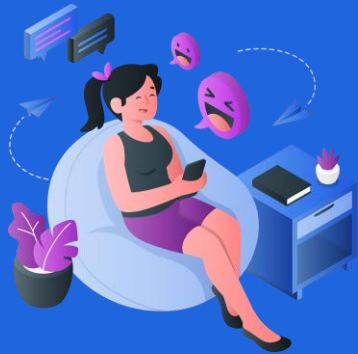
FERRAMENTAS DE SEGURANÇA DE DADOS PARA SISTEMAS IOT



Aluno: Rhuan Martins de Souza
Orientador: Esdras Nicoletto da Cunha

Introdução

- Domótica e seus benefícios
- Dispositivos Internet das coisas (IoT)





Justificativa

Até que ponto é seguro adicionar
diversos equipamentos diretamente
a uma rede ?



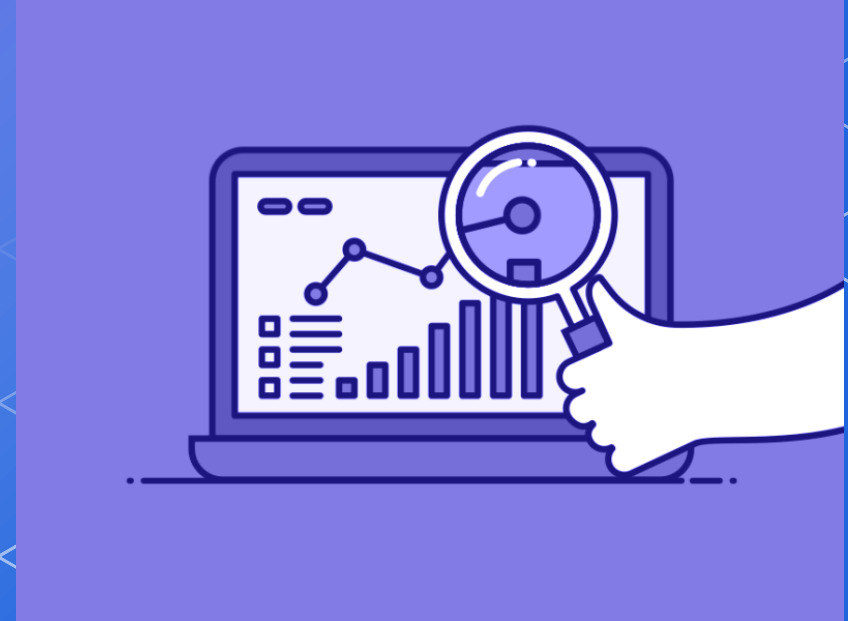
Objetivos

- Bom funcionamento do sistema web server
- Boa implementação do design da rede do sistema
- Tráfego de dados seguro entre os sensores, atuadores e demais dispositivos do sistema



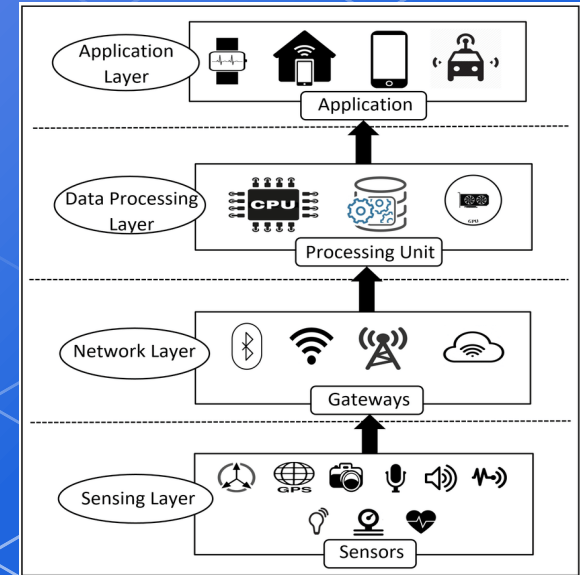
Pesquisa Bibliográfica

- Estrutura de sistemas IoT
- Ataques utilizados em IoTs
- Meios de proteção aplicáveis



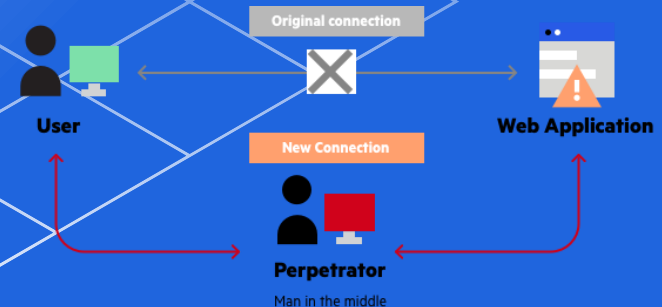
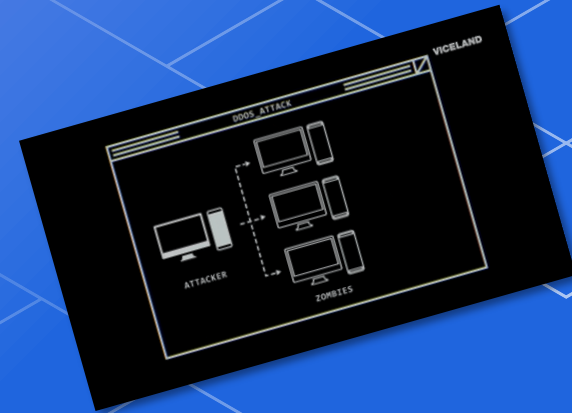
Estrutura do sistema

- Interface IHM
- Web-server/programações
- Transmissão e recebimento dos dados
- Sensores e atuadores



Ataques utilizados em IoTs

- Sequestro da rede
- Acesso a informações pessoais
- Danificar máquinas e equipamentos conectados a rede



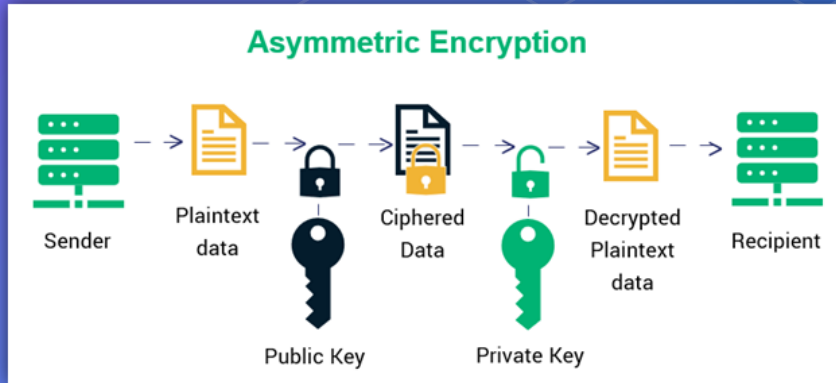
Proteções aplicáveis

- Boas praticas de Design de Rede
- Mecanismos de segurança



Proteções aplicáveis

- Conexão com protocolo TLS (Transport Layer Security)

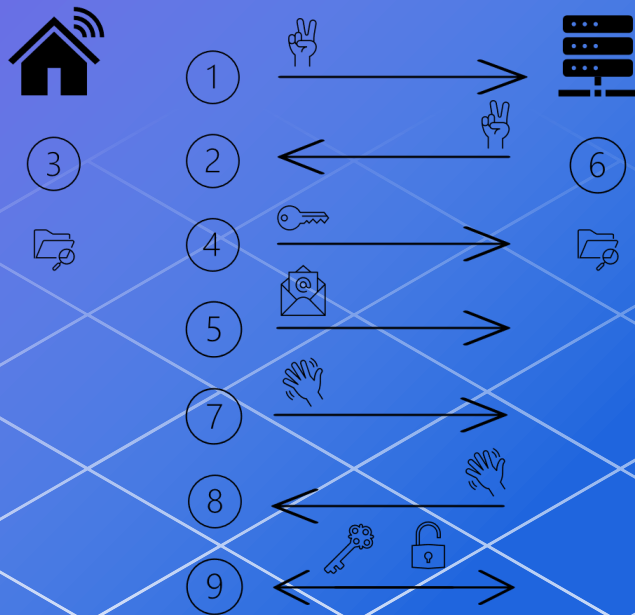


Proteções aplicáveis

- TLS Handshake

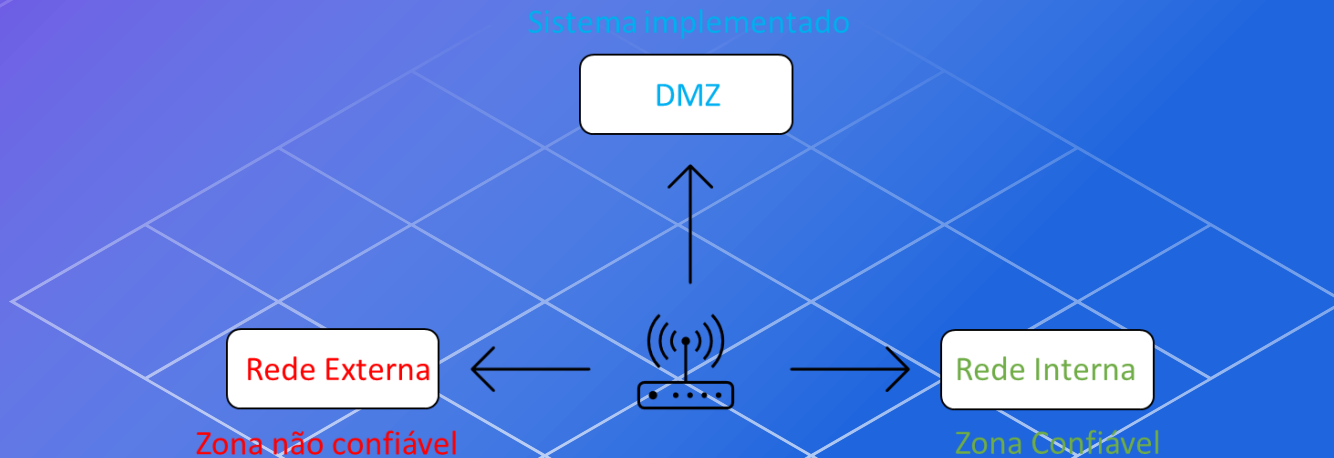
MQTT Client

MQTT Broker



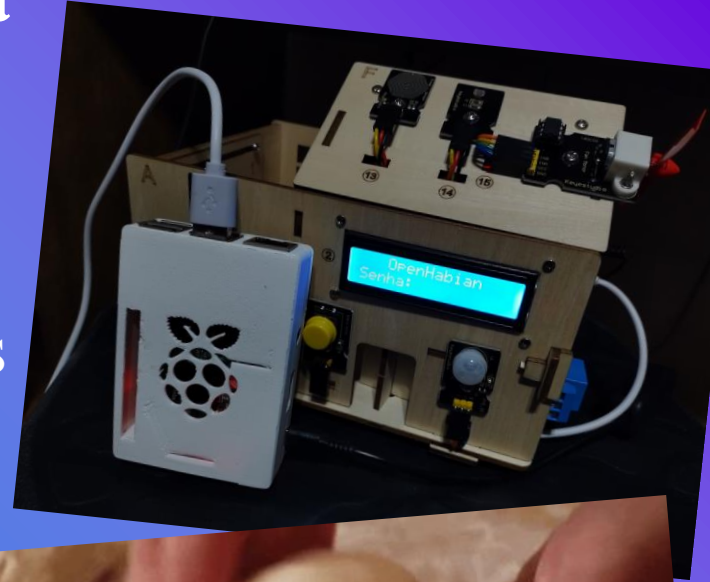
Proteções aplicáveis

- Demilitarized Zone (DMZ)

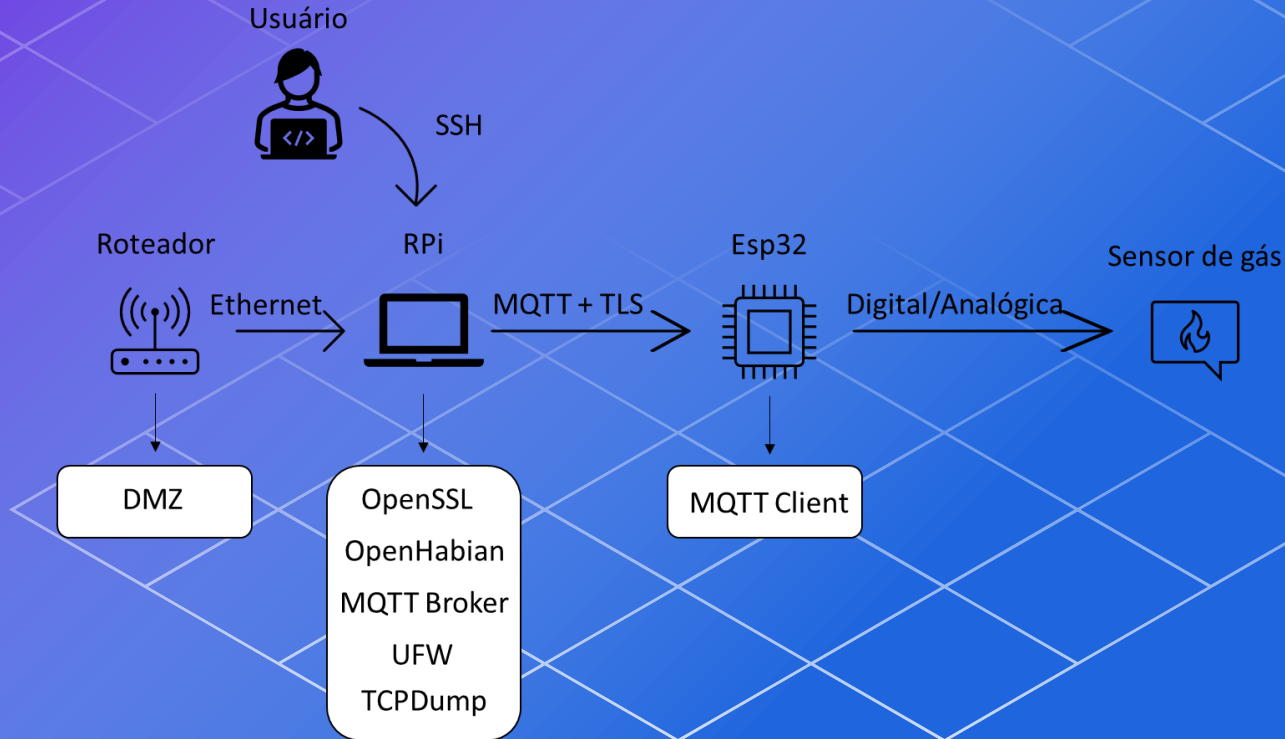


Metodologia

- Equipamentos e estrutura implementada
- OpenHABian
- MQTT(Message Queuing Telemetry Transport) e TLS
- Demilitarized Zone




Equipamentos e estrutura do sistema



OpenHABian

- Etcher
- SSH
- Web server

Sensor_gas



Cozinha

String

890

Tags

Measurement

Gas

Semantic Classification

class

Point_Measurement

relatesTo

Property_Gas

Metadata

[Add Metadata](#)

Channel Links

Sensor_gas

Cozinha

mqtttopic:bdeb50b078:Sensor_gasCanal_esp32

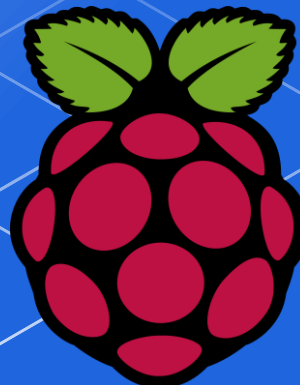
ONLINE >

[Add Link](#)

MQTT e TLS

```
1.sudo apt-get update  
2.sudo apt-get install mosquitto  
3.sudo apt-get install mosquitto-clients  
4.sudo apt clean  
5.mosquitto -v  
6.netstat -at
```

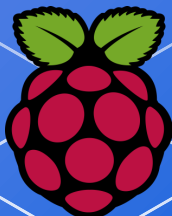
```
1.sudo apt-get install ufw  
2.sudo systemctl start ufw  
3.sudo ufw allow 8883/tls  
4.sudo ufw reload  
5.sudo ufw status
```



MQTT e TLS

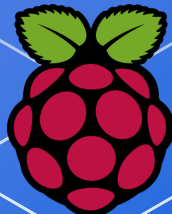
```
1.sudo apt-get install openssl
2.openssl genrsa -des3 -out ca.key 2048
3.openssl req -new -x509 -days 1833 -key ca.key -out ca.crt
4.openssl genrsa -out server.key 2048
5.openssl req -new -out server.csr -key server.key
6.openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out server.crt -days 360
```

```
"listener 8883
cafile /etc/mosquitto/certs/ca.crt
certfile /etc/mosquitto/certs/server.crt
keyfile /etc/mosquitto/certs/server.key
tls_version tlsv1.2"
```



DMZ – Zona Desmilitarizada

1.Modificar diretamente no roteador local



DMZ

Status atual do DMZ ☒ Ativar ☐ Desativar

Endereço IP da estação DMZ:

Salvar

Resultados obtidos

1. netstat -at

```
openhavian@openhavian:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:1883             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:9001             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:microsoft-ds    0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ssh              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:netbios-ssn        0.0.0.0:*               LISTEN
tcp        0      0 :::0.100:1883           :::0.102:57480          ESTABLISHED
tcp        0      0 :::0.100:1883           :::0.100:40056          ESTABLISHED
tcp6       0      0 [::]:1883               [::]:*                  LISTEN
```

1. sudo tcpdump -A -s0 port 1883

```
E..(..@.....d...f[...w..Y..P....5..
21:24:58.862216 IP 192.168.0.102.53971 > 192.168.0.100.1883: Flags [P.], seq 1468:1539, ack 12, win 5733, length 71
E..o.G....9'...f...d...[.Y.E..w.P..e...l...myHome/gasSensor590...l...myHome/gasSensor589l...myHome/gasSensor592
21:24:58.862290 IP 192.168.0.100.1883 > 192.168.0.102.53971: Flags [.], ack 1539, win 63925, length 0
E..(..@.....d...f[...w..Y..P....5..
21:24:58.863043 IP 192.168.0.100.1883 > 192.168.0.102.53971: Flags [P.], seq 12:14, ack 1539, win 63925, length 2
E...@.....d...f[...w..Y..P....7....
21:24:58.901824 IP 192.168.0.102.53971 > 192.168.0.100.1883: Flags [P.], seq 1539:1562, ack 14, win 5731, length 23
E..?.H....9V...f...d...[.Y....w.P..c!...l...myHome/gasSensor607
21:24:58.943458 IP 192.168.0.100.1883 > 192.168.0.102.53971: Flags [.], ack 1562, win 63925, length 0
E..(..@.....d...f[...w..Y..P....5..
21:24:59.460300 IP 192.168.0.102.53971 > 192.168.0.100.1883: Flags [P.], seq 1562:1585, ack 14, win 5731, length 23
E..?.I....9U...f...d...[.Y....w.P..c....l...myHome/gasSensor618
```

Resultados obtidos

- Configuração do TLS pela porta 8883

```
openhabian@openhabian:/etc/mosquitto/certs $ sudo tcpdump -A -s0 port 8883
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
2:29:47.596280 IP 192.168.0.103.51292 > 192.168.0.100.8883: Flags [P.], seq 3491
48662:3491148714, ack 1964191089, win 4411, length 52
...\\.....+....g...d.\"....vu.-qP.;D...../.....e.l..C).... JP..y|...n?...nH.P
...\"3G..5.
2:29:47.596354 IP 192.168.0.100.8883 > 192.168.0.103.51292: Flags [.], ack 52, w
in 63680, length 0
...(.@.@.2....d...g\"...\\u.-q....P....6..
2:29:48.101051 IP 192.168.0.103.51292 > 192.168.0.100.8883: Flags [P.], seq 52:1
04, ack 1, win 4411, length 52
...\\.....+....g...d.\".....u.-qP.;...../.....f.....r}.....\\I.Y9.....s
1.4.....
2:29:48.101159 IP 192.168.0.100.8883 > 192.168.0.103.51292: Flags [.], ack 104,
win 63680, length 0
...(.@.@.2....d...g\"...\\u.-q....P....6..
2:29:48.604680 IP 192.168.0.103.51292 > 192.168.0.100.8883: Flags [P.], seq 104:
56, ack 1, win 4411, length 52
...\\.....+....g...d.\".....u.-qP.;)...../.....g~.&xn.....
```

Considerações finais

- Benefícios em segurança e privacidade
- Integração de equipamentos
- Sistema eficiente e de baixo custo



Limitações

- Falta de um firewall físico
- Complexidade e custos
- Ataques de força bruta



Obrigado!

dúvidas?

rhuan.m@aluno.ifsp.edu.br