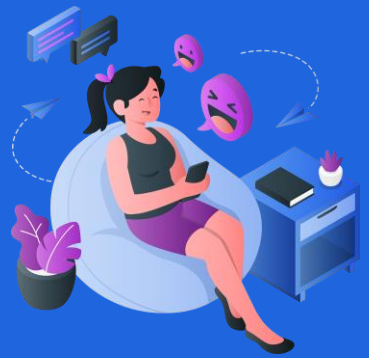
FERRAMENTAS DE SEGURANÇA DE DADOS PARA SISTEMAS IOT

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

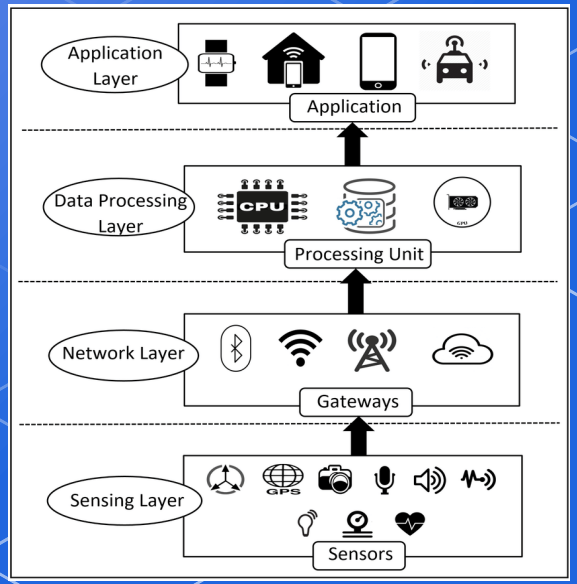
- Bom funcionamento do sistema web server
- Boa implementação do design da rede do sistema
- Tráfego de dados seguro entre os sensores, atuadores e demais dispositivos do sistema

Pesquisa Bibliográfica

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

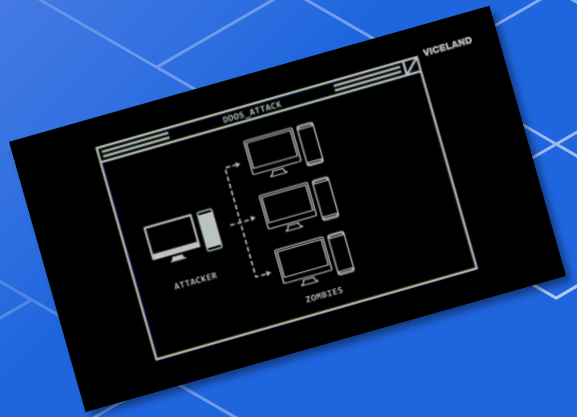
Estrutura do sistema

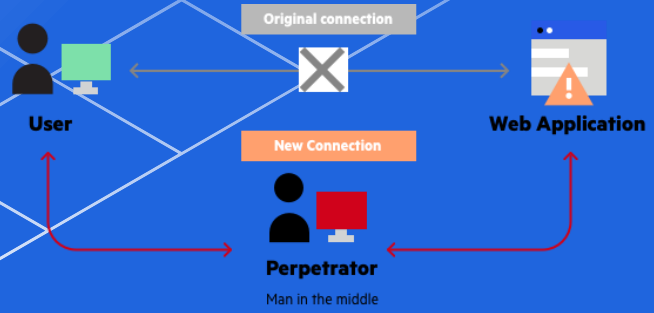
- Inteface IHM
- Web-server/programações
- Transmissão e recebimento dos dados
- Sensores e atuadores



Ataques utilizados em IoTs

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



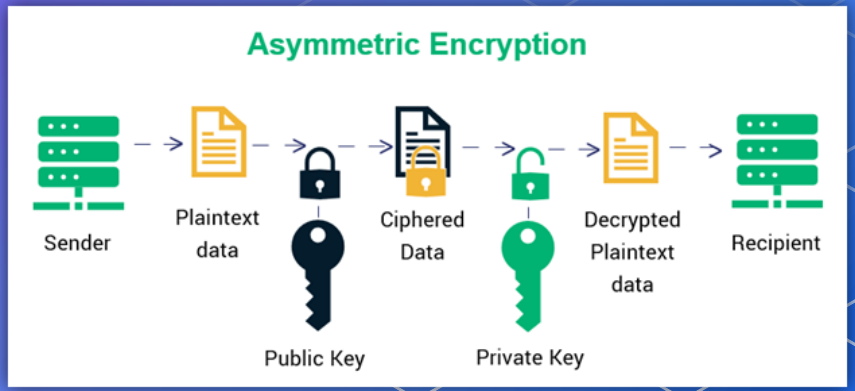


Proteções aplicáveis

- Boas praticas de Design de Rede
- Mecanismos de segurança

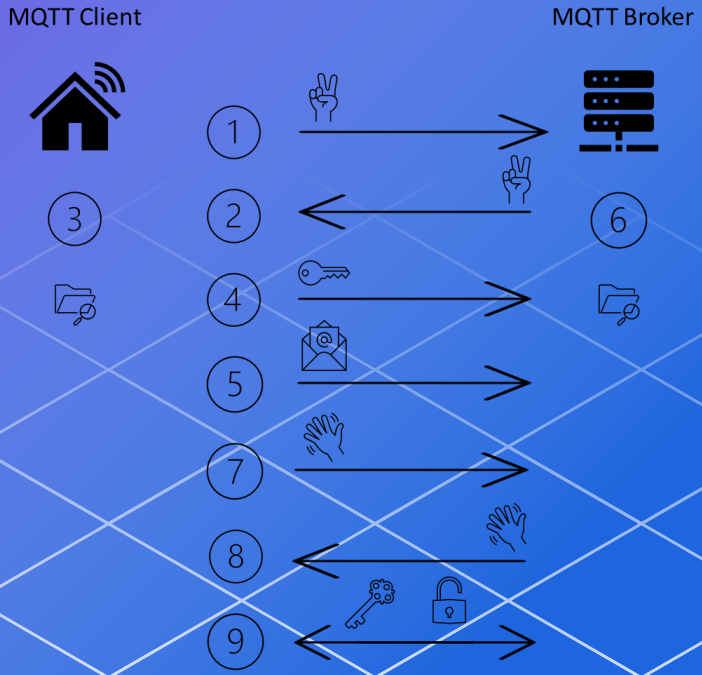
Proteções aplicáveis

- Conexão com protocolo TLS (Transport Layer Security)



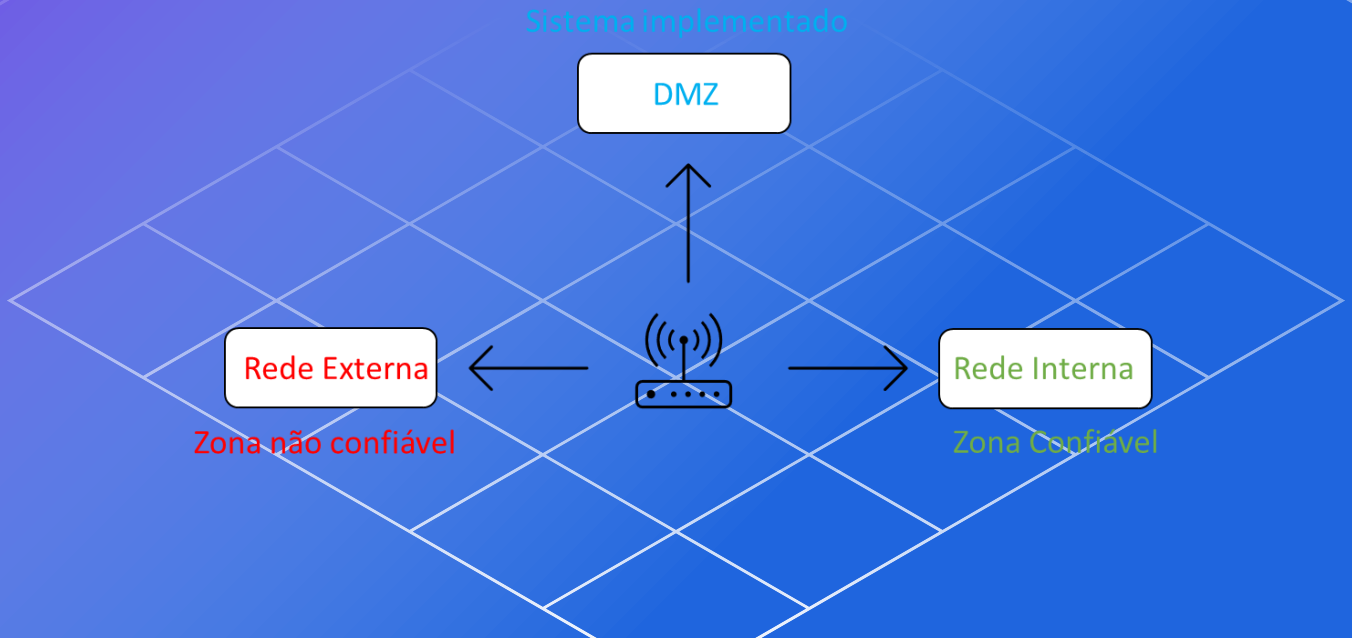
Proteções aplicáveis

- TLS Handshake



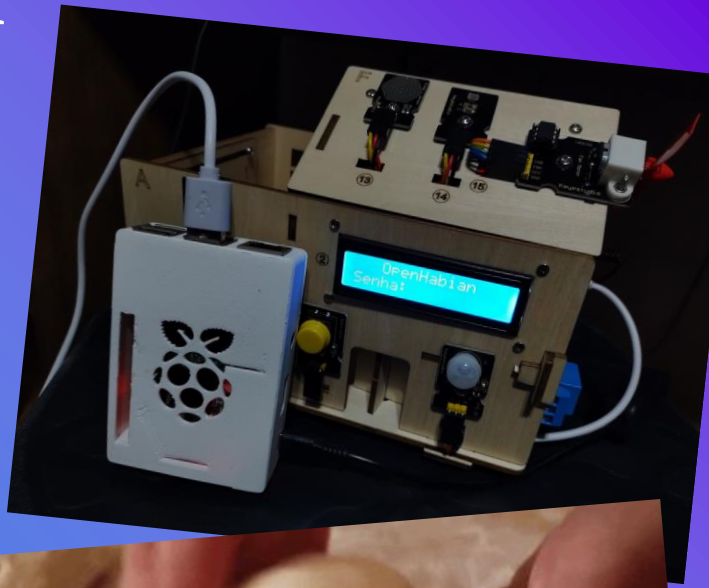
Proteções aplicáveis

- Demilitarezed Zone (DMZ)

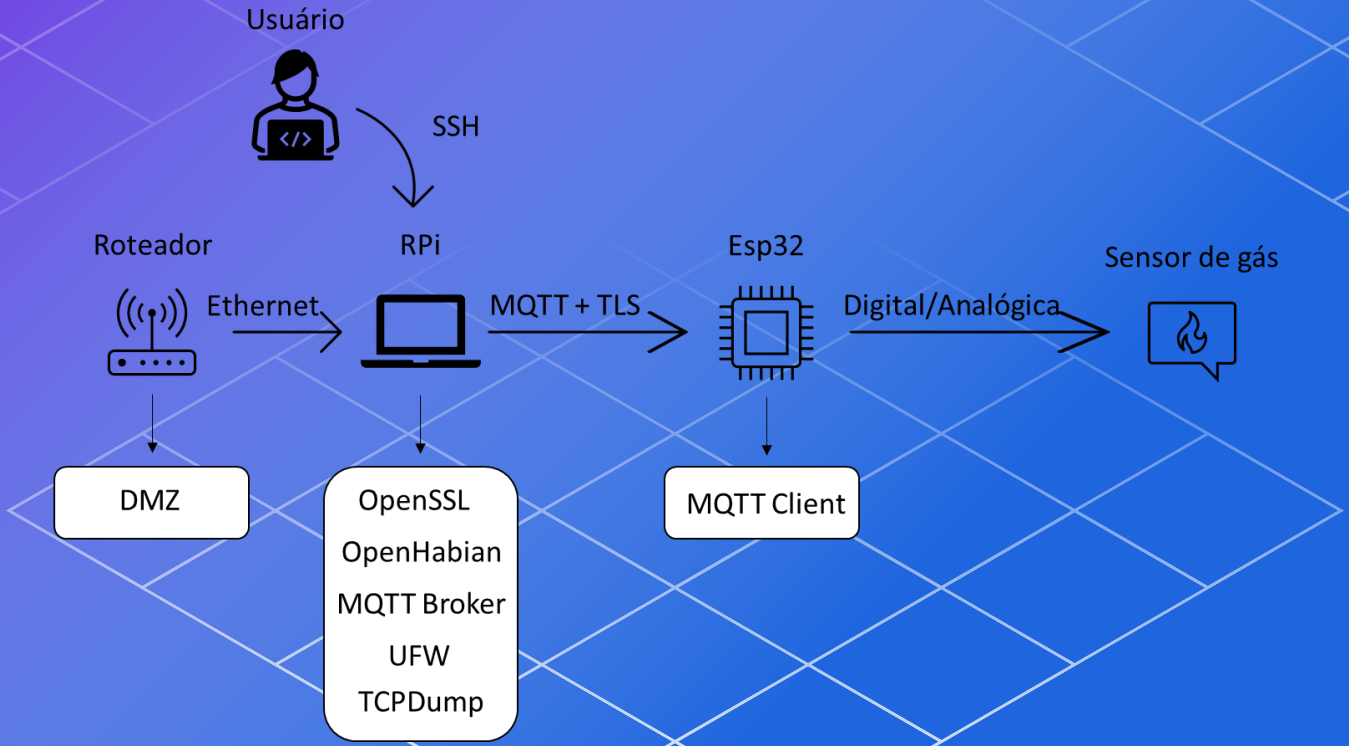


Metodologia

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

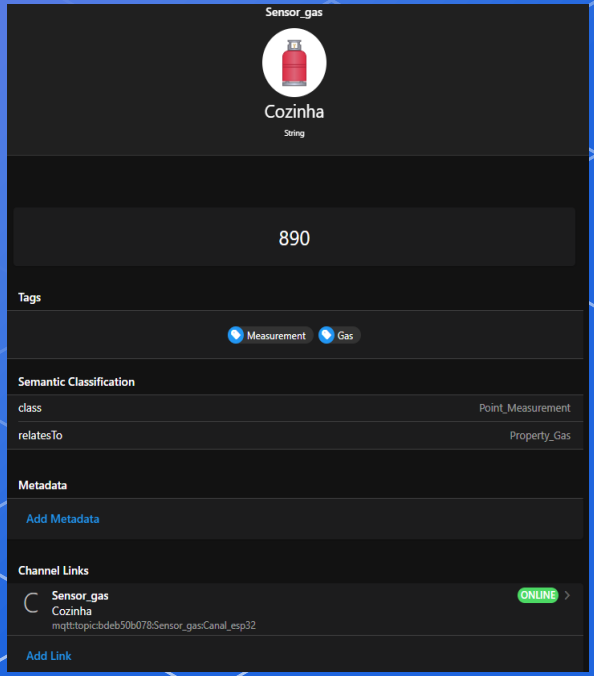


Equipamentos e estrutura do sistema



OpenHABian

- Etcher
- SSH
- Web server



MQTT e TLS

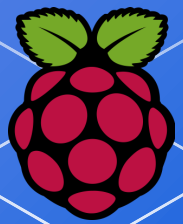
```
1.sudo apt-get update
2.sudo apt-get install mosquitto
3.sudo apt-get install mosquitto-clients
4.sudo apt clean
5.mosquitto -v
6.netstat -at
```

```
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

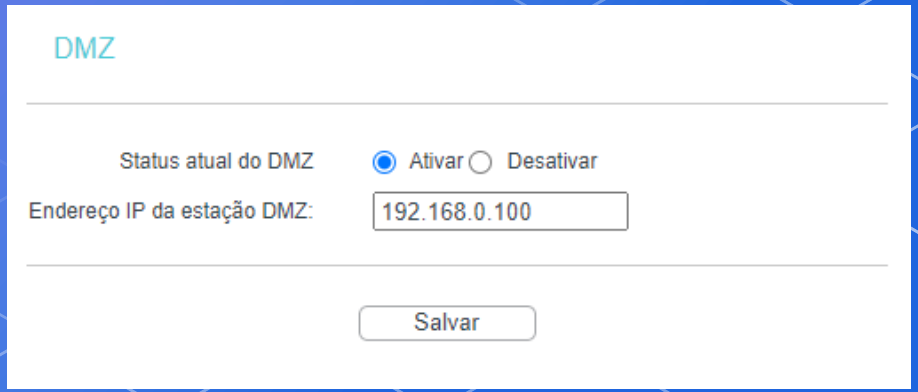
```
1.sudo apt-get install openssl
2.openssl genrsa -des3 -out ca.key 2048
3.openssl req -new -x509 -days 1833 -key ca.key -out ca.crt
4.openssl genrsa -out server.key 2048
5.openssl req -new -out server.csr -key server.key
6.openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -
CAcreateserial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



Resultados obtidos

1.netstat -at

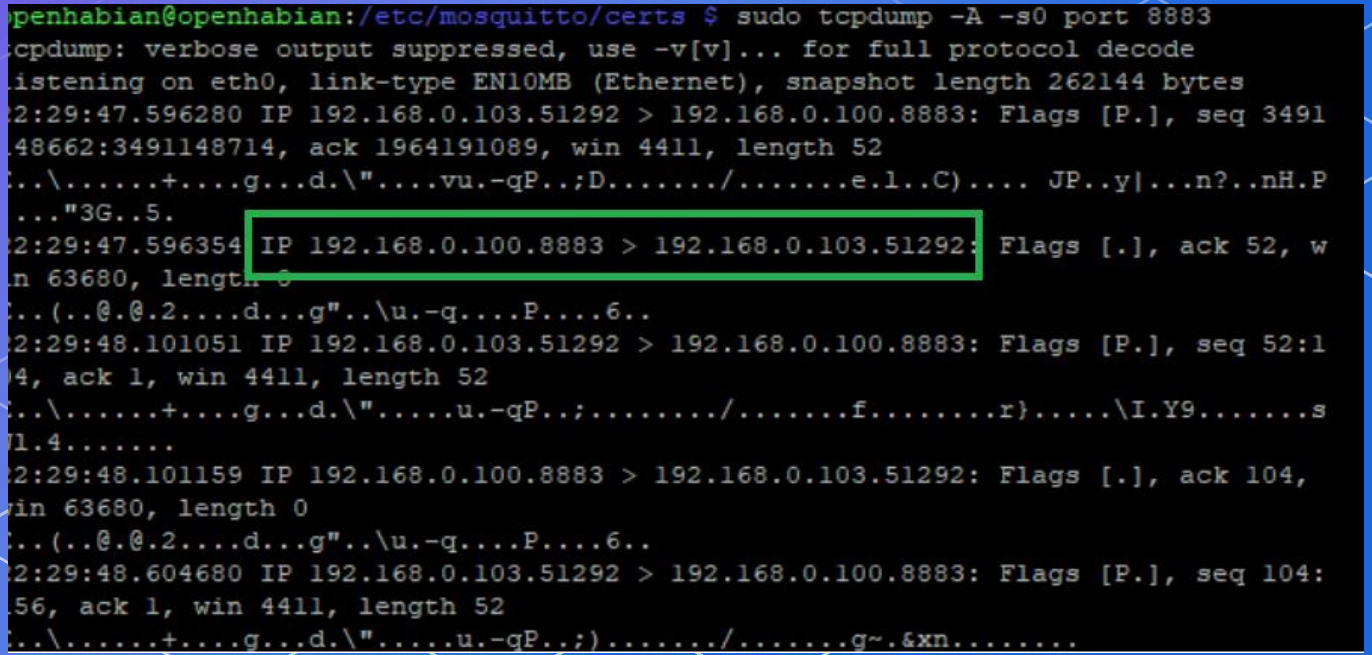
```
openhabian@openhabian:~ $ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:1883            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:9001            0.0.0.0:*  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

1.sudo tcpdump -A -s0 port 1883

```
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....1...myHome/gasSensor590..1...myHome/gasSensor5891...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!...1..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....1...myHome/gasSensor618
```

Resultados obtidos

- Configuração do TLS pela porta 8883



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