PUE 5TH DAY MADRID 2018

#PUEDAY18

WORKSHOP DE CLAUSURA: IOT & CIBERSEGURIDAD

16:45h a 17:45h

Ciberseguridad en entornos IoT

Ponente: Ramon de la Rosa Falguera – IT Manager at PUE

Networking Academy

Agenda

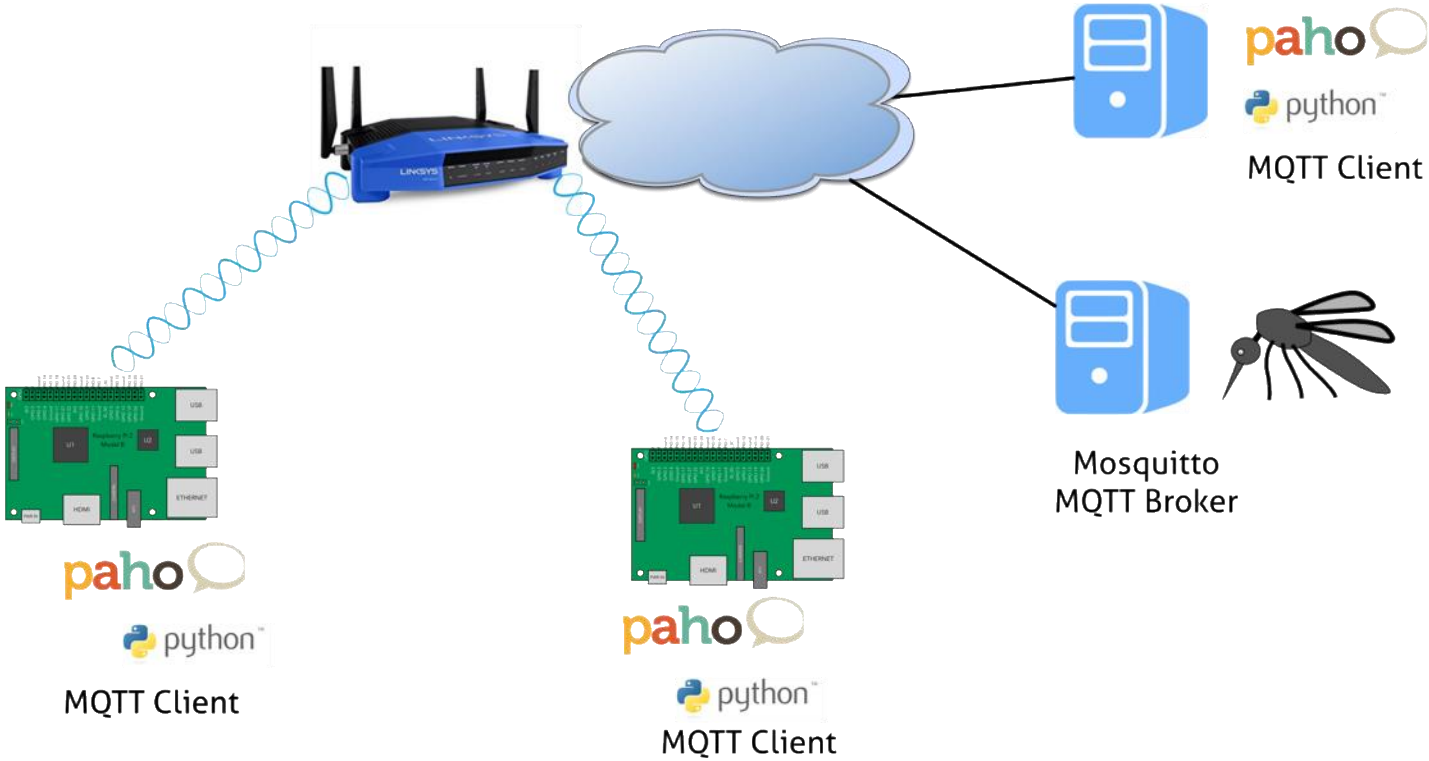
- Prototipo IoT
- Protocolo MQTT
- Debilidades prototipo IoT
- Segurización del prototipo IoT

Prototipo IoT

Lego Smart Home

- **Control de luz**
- **Apertura automática de puerta**
- **Medición automática temperatura, humedad, luz**
- **Tele timbre**

MQTT Prototipo Smart Home



Networking Academy

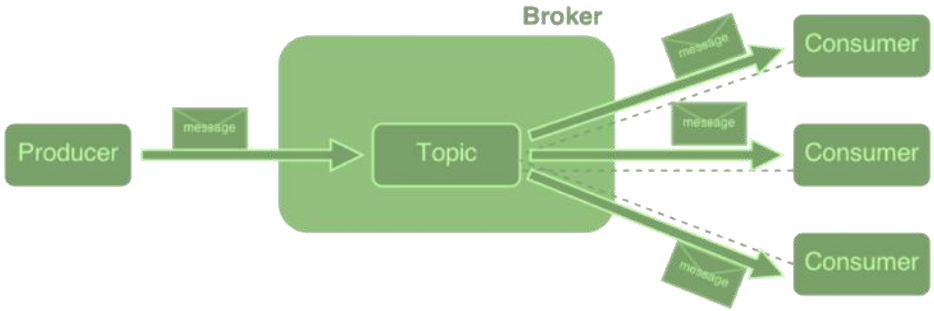
pue IMPULSANDO EL CONOCIMIENTO TIC CUALIFICADO

MQTT

Protocolo IoT M2m

Message Queuing Telemetry Transport

MQTT


Broker
Producer
message
Topic
message
message
message
Consumer
Consumer
Consumer


mosquitto

MQTT

Sensores /lego/out		Actuadores /lego/in	
/lego/out/temp	Temperatura en grados	/lego/in/door	1 Abrir 0 Cerrar
/lego/out/hum	Humedad %	/lego/in/led	1 On 0 Off
/lego/out/ldr	0-1023 LDR	/lego/in/take_photo	1 Tomar una foto
/lego/out/doorbell	1 Ring 0 Stop Ring		
/lego/out/photo	PiCam en Base64		

AUDITORIA DE SEGURIDAD

Debilidades sistema Iot

- Protocolos en comunicación IP, WIFI
- Dispositivos IoT (todas las debilidades del SO)
- Protocolo MQTT
- Configuraciones por defecto

Debilidades 2

Redes Wifi	Dispositivos IoT	MQTT
Captura del tráfico	Recursos limitados	Suplantación de identidad
Accesos no autorizados	Exploits Sistema Operativo	Generación de datos falsos
DoS	Acceso no autorizado	Captura de información

SECURIZACIÓN MQTTT

TLS

Autenticación de cliente

Autorización

MQTT Default config

```
▶ Frame 859: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
▶ Ethernet II, Src: Apple_41:d8:63 (40:6c:8f:41:d8:63), Dst: 62:38:e0:d7:63:43 (62:38:e0:d7:63:43)
▶ Internet Protocol Version 4, Src: 192.168.1.111, Dst: 35.196.255.71
▶ Transmission Control Protocol, Src Port: 55637, Dst Port: 1883, Seq: 3237874071, Ack: 454243106, Len: 19
▼ MQ Telemetry Transport Protocol
  ▼ Publish Message
    ▼ 0011 0000 = Header Flags: 0x30 (Publish Message)
        0011 .... = Message Type: Publish Message (3)
        .... 0... = DUP Flag: Not set
        .... .00. = QOS Level: Fire and Forget (0)
        .... ...0 = Retain: Not set
      Msg Len: 17
      Topic: /lego/out/door
      Message: 1
```

```
0000  62 38 e0 d7 63 43 40 6c  8f 41 d8 63 08 00 45 00   b8..cC@l .A.c..E.
0010  00 47 00 00 40 00 40 06  00 00 c0 a8 01 6f 23 c4   .G..@.@. .....o#.
0020  ff 47 d9 55 07 5b c0 fe  09 97 1b 13 33 22 80 18   .G.U.[.. ....3"..
0030  10 27 e5 5c 00 00 01 01  08 0a 38 22 74 67 07 a1   .'.\.... ..8"tg..
0040  27 da 30 11 00 0e 2f 6c  65 67 6f 2f 6f 75 74 2f   '.0.../l ego/out/
0050  64 6f 6f 72 31                                    door1
```

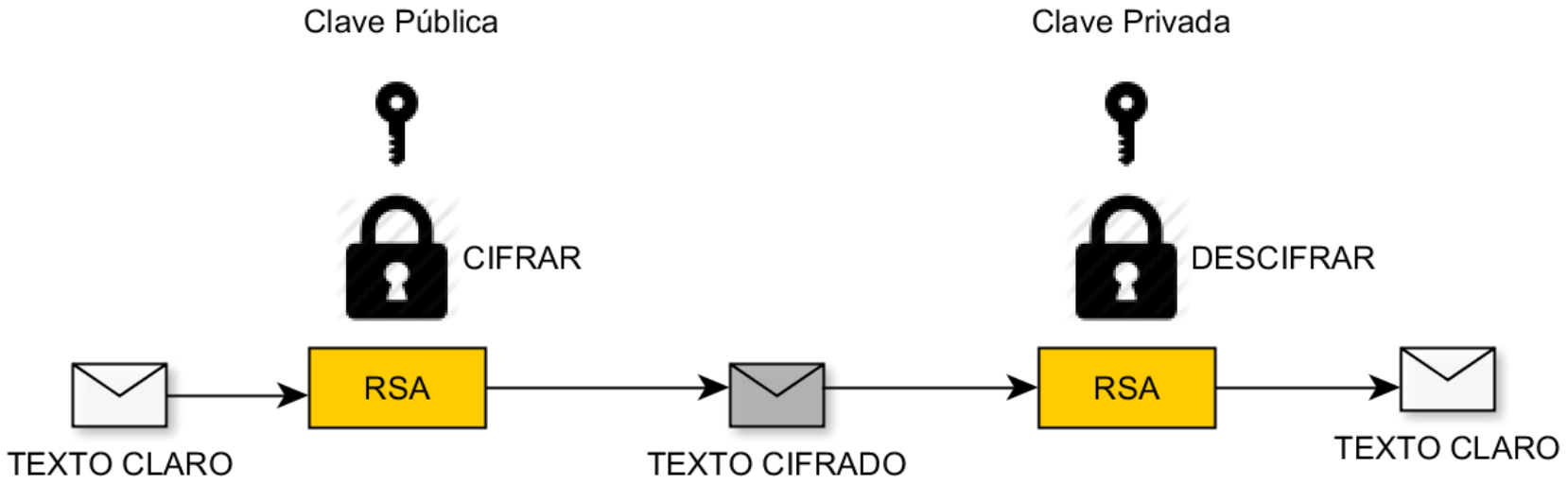
Networking Academy

IMPULSANDO EL CONOCIMIENTO TIC CUALIFICADO

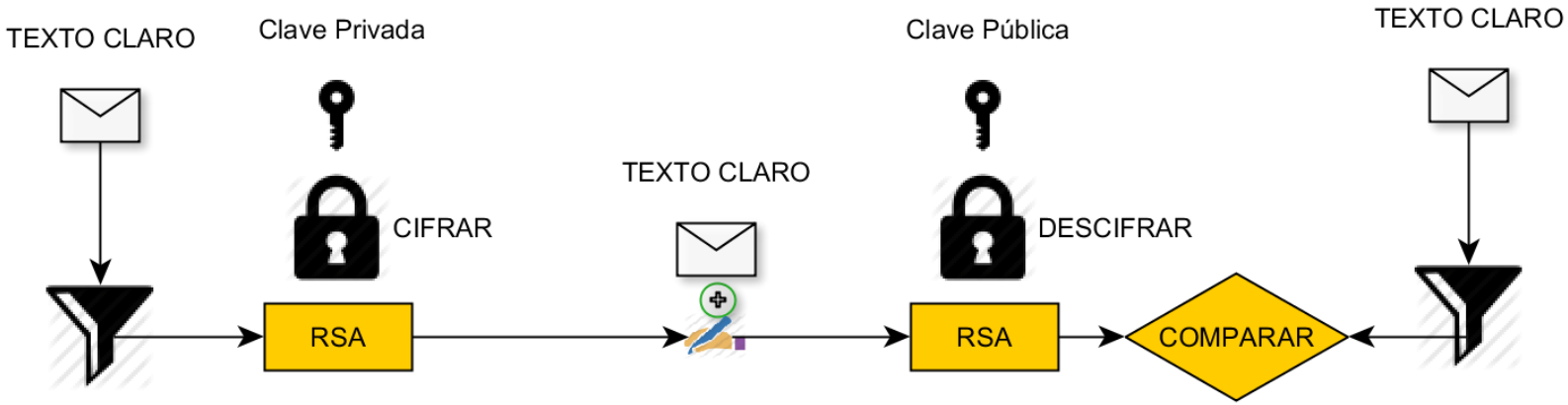
Cifrado MQTT (TLS)

- Idéntica a la seguridad aplicada en la protección de páginas web HTTPS
- Basado en el uso de certificados digitales

RSA Cifrado


Clave Pública
Clave Privada
CIFRAR
DESCIFRAR
RSA
RSA
TEXTO CLARO
TEXTO CIFRADO
TEXTO CLARO

RSA Firma


TEXTO CLARO
Clave Privada
CIFRAR
RSA
TEXTO CLARO
Clave Pública
DESCIFRAR
RSA
COMPARAR
TEXTO CLARO


Digest +
RSA Sig CA
Private Key
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
c0:50:f9:2d:93:5d:b6:9c
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=ES, ST=Barcelona, L=Barcelona, O=PUEDAY18, CN=MYCA
Validity
Not Before: Apr 8 23:02:44 2018 GMT
Not After : Apr 6 23:02:44 2023 GMT
Subject: C=ES, ST=Barcelona, L=Barcelona, O=PUEDAY18, CN=MYCA
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (4096 bit)
Modulus:
00:b1:40:27:a6:38:8b:92:5c:2b:54:5c:64:17:24:
.....
16:c6:ab
Exponent: 65537 (0x10001)
Pub Key
X509v3 extensions:
X509v3 Subject Key Identifier:
A1:98:82:8F:18:71:12:D0:3A:DA:3E:53:18:EF:29:FB:D4:38:D5:55
X509v3 Authority Key Identifier:
keyid:A1:98:82:8F:18:71:12:D0:3A:DA:3E:53:18:EF:29:FB:D4:38:D5:55
X509v3 Basic Constraints:
CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
54:ea:2a:b4:2a:f3:c6:46:43:aa:1f:a4:62:f0:35:cd:64:14:
.....
9b:a0:dc:82:12:56:ec:9e:6a:df:f2:d2:48:1c:79:56:1e:40:
6a:a3:53:fa:cb:98:4a:4a

Habilitar TLS MQTT

1. Creación de la CA
2. Certificado para el servidor Mosquitto
3. Distribuir certificados
4. Modificar configuración daemon Mosquitto
5. Modificar aplicaciones cliente MQTT

Habilitar autenticación basada en x509

1. Crear certificados clientes
2. Distribuir certificados
3. Modificar configuración servidor mosquitto
4. Modificar aplicaciones cliente mqtt

Control de acceso

	RPI00	RPi11	WebServer
/lego/out/temp	W	R	R
/lego/out/hum	W	R	R
/lego/out/ldr	W	R	R
/lego/out/doorbell	W	R	R
/lego/out/photo	W	R	R
/lego/in/door	R	RW	RW
/lego/in/led	R	RW	RW
/lego/in/take_photo	R	-	-

GitHub repo

https://github.com/rdelaros/IoT_CiberSecurity_PUEDAY18

BARCELONA – MADRID

www.pue.es

¡Gracias!

#PUEDAY18

educación@pue.es

93 206 02 49

PUE 5TH DAY MADRID 2018

ORACLE ACADEMY

cloudera ACADEMIC PARTNER

Microsoft Imagine Academy

vmware IT ACADEMY

Linux Professional Institute

RED HAT ACADEMY redhat.

cisco Networking Academy