Analisis de la seguridad de datos aplicado a sistemas ciberfisicos

Ramiro Serrano
Escuela Superior Politécnica
del Litoral
Guayaquil, Ecuador
Email: rsserran@espol.edu.ec

Keywords— Ataques, Red de Sensores, Ciberfisico, Seguridad

1. Introduction

Debido al desarrollo de los sistemas embebidos, áreas de desarrollo como agricultura, acuicultura, seguridad, domótica han visto grandes beneficios, sin embargo, estas áreas manejan información sensible por lo que la seguridad de esta data es importante, asimismo la integridad, confiabilidad y disponibilidad de sistema que maneja la información es tan importante como la red que recopila los datos, para esto es imperante establecer reglas de seguridad al servidor que almacena los datos.
Otro aspecto para notar es que los sistemas ciberfisicos al manejar dispositivos que transmiten datos como los son zigbee o esp32, pueden verse potencialmente afectados por inyección de software, siendo de esta manera que la información podría ser manejada o enviada hacia un destino diferente del deseado por el cliente.
Otro aspecto de seguridad es que los resultados de algunos sensores pueden ser manipulados de forma fisica, por lo que tambien es importante notar como un aspecto de seguridad aplicar redundancia al ubicar los sensores y redundancia para la recopilacion de los datos, de esta manera podriamos reducir la recepcion de datos erroneos accidentales.

2. Objectivos

Analizar el estado de la seguridad implementada en redes de sensores y los servidores de almacenamiento de datos a los que estos se conectan.

3. Trabajos relacionados

Carlos Mario Paredes habla en su paper sobre el procedimiento para el diseño de sistemas ciberfisicos enfatizando la seguridad de la informacion y como prevenir ciertos ataques[1].
Asimismo, Catalina aranzazu presenta un paper explicando en detalle los tipos de ataques que puede recibir una red, junto a esto tambien presenta ciertas normativas de seguridad que se pueden implementar para su prevencion[2].
Por ultimo tenemos el trabajo realizado por M. Segovia, este trabajo muestra con mayor detalle aun capa por capa como se puede prevenir ataques y como robustecer la seguridad de una red que usa sensores como dispositivo de toma de datos[3].

4. Metodologia Experimental

Para este proyecto, lo que se planea implementar es una red de comunicacion entre dispositivos IoT de una red domotica y un raspberry pi, asimismo, se establecera una conexion entre el raspberry y telegram para facilitar el manejo de dichos dispositivos, teniendo en consideracion medidas de seguridad en los puertos usados.
a continuacion se presenta un ejemplo de un potencial esquematico que se va a usar:

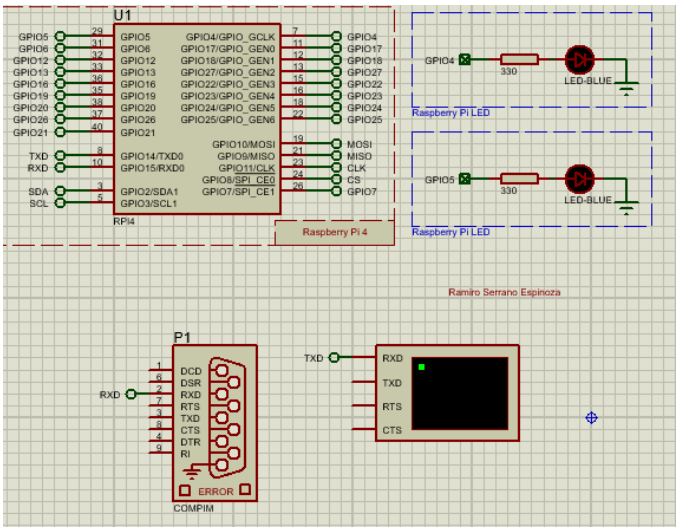

Figure 1. Esquematico de la red receptora de informacion.

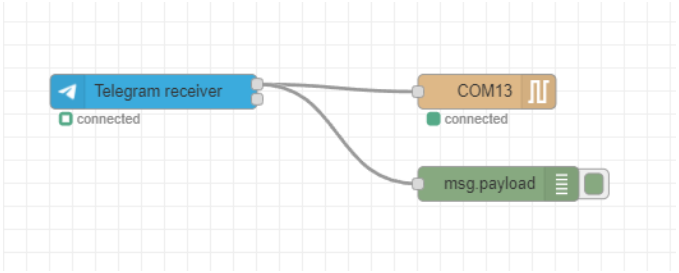

Figure 2. Esquematico de node-red.

4.1. Equipos usados

1) Raspberry pi 4
2) Compim
3) Virtual terminal
4) Leds
5) Resistencias

Dispositivo	Voltaje[V]	Corriente[mA]
Raspberry pi 4 idle	5	25
Raspberry pi 4 active	5	250
led	2	20

TABLE 1. CONSUMO DE DISPOSITIVOS

5. Resultados

El diseño del proyecta en mantener seguro un canal de comunicacion entre dispositivos en una red local, por lo que en este caso se uso una conexion entre Telegram con Node-Red y Node-Red con la simulacion en proteus. Dado que la conexion entre telegram y Node-Red requiere conocer un id unico del chat entre el usuario y el bot que envia el mensaje, usaremos ese mismo id como credencial de verificacion en el raspberry, como resultado obtenemos una comunicacion que si llegase el puerto a ser usado o atacado por un tercero, al no enviar el mensaje del id valido, no se podra activar ningun dispositivo en la red receptora.

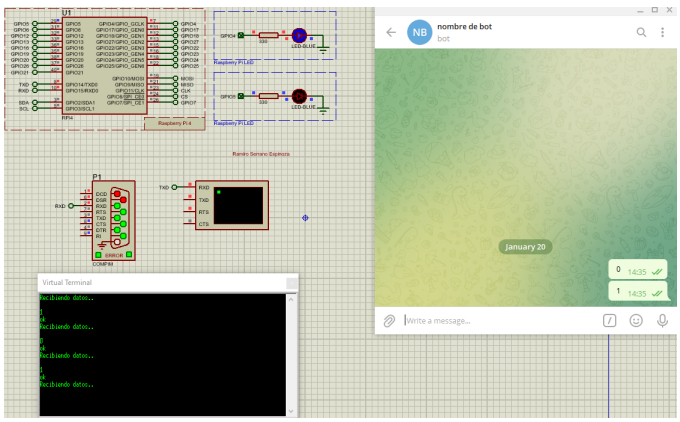

Figure 3. Resultados de la simulacion.

6. Conclusiones

- Se logro establecer comunicacion segura entre los dispositivos al verificar credenciales en la trama del mensaje transmitido.
- Se implmento una red domotica controlable desde una aplicacion de mensajeria, lo cual nos permitio hacer uso de los dispositivos sin necesidad de encontrarnos fisicamente cerca del microcontrolador.

7. Referencias

[1]C. M. . Paredes Valencia, PROCEDIMIENTO DE DISEÑO DE SISTEMAS CIBERFÍSICOS DE TIEMPO REAL TOLERANTES A ATAQUES CIBERNÉTICOS, EIEI ACOFI, ago. 2019.

[2]C. Aranzazu, https://www.icesi.edu.co/revistas/index.php /sistemas_telematica/article/download/1006/1031/

[3] M. Segovia, https://www.colibri.udelar.edu.uy/jspui/bitstream/ 20.500.12008/19019/1/2078.pdf

8. Enlace Github

https://github.com/rsserran