Ciberseguridad en Redes Industriales

M. Luna[(1)]

mluna@inti.gob.ar

[(1)]Laboratorio de Ciberseguridad Industrial-Dto. Validación de Dispositivos y Sistemas Electrónicos-DT Electrónica-SOEyE-GOSI-INTI

Palabras Clave: I4.0; IIoT; Ciberseguridad; MQTT.

INTRODUCCIÓN

La Industria 4.0 se basa en un modelo de industria inteligente que adopta tecnologías habilitadoras para su sustento. Dentro de estas tecnologías habilitadoras toman relevancia la Internet industrial de las cosas (IIoT) y la Ciberseguridad.

En el marco de la actual transformación digital, se da un incremento en la vinculación entre redes industriales de Tecnología de Operaciones (OT) y redes públicas. Este hecho incrementa las vulnerabilidades a las que las redes OT están expuestas dado que dejan de estar circunscriptas a un entorno aislado netamente industrial.

MQTT es un protocolo de comunicación Machine to Machine (M2M) que se convirtió en uno de los estándares para el intercambio de datos en la IIoT por su facilidad de implementación y bajo uso de recursos. Utiliza una estructura de “publicar/suscribir” de la que forman parte clientes (PLCs, sensores, etc) y un broker (o servidor) que tiene la función de ser un nexo intermediario para el intercambio de información entre los clientes. Esta tecnología brinda una solución escalable y de bajo costo para la incorporación de dispositivos a las redes OT.

OBJETIVOS

Establecer mecanismos de seguridad en comunicaciones basadas en protocolo MQTT en redes OT para permitir un intercambio de datos de manera segura, disminuyendo la probabilidad de ciberataques. Definir los mecanismos adecuados en función de la criticidad de la información intercambiada y la capacidad de procesamiento de los dispositivos y el ancho de banda disponible.

DESARROLLO

Se implementaron y evaluaron distintos mecanismos de seguridad, estableciendo comunicaciones entre dispositivos clientes (PC, celulares y microprocesadores) y un broker MQTT Mosquitto (OpenSource) instalado en una microcomputadora Raspberry Pi 3 (Figura 1). [1]

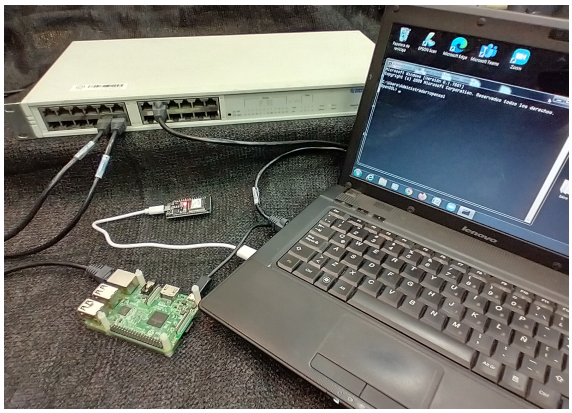

Figura 1 – Hardware utilizado

Las comunicaciones de datos utilizando protocolo MQTT entre clientes y brokers pueden realizarse sin ninguna limitación cuando no se utilizan mecanismos de protección de la información en la publicación o recepción de la misma. Para publicar información el cliente sólo debe definir un tópico y enviar los datos al broker. Por el lado del suscriptor, la única condición que debe tener un cliente para conectarse y recibirla es conocer el tópico de publicación (en rigor existen maneras para recibir los mensajes aún desconociendo los tópicos mediante el uso de “wildcards” o comodines).

Se pueden establecer tres niveles de seguridad en el envío y recepción de datos además del modo de operación básico mencionado. Conforme va aumentando el grado de protección de estos niveles frente a ciberataques, van aumentando el grado de complejidad en su implementación y los recursos utilizados, tanto de volumen de procesamiento como en el uso de ancho de banda.

El nivel más básico de protección implementado fue la definición de usuarios y claves en los brokers. De esta forma se limita la posibilidad de conexión de cualquier dispositivo sin identificación. Los clientes deben conocer el usuario y clave de conexión para poder estabelecer la comunicación, tanto para la

publicación como para la suscripción de mensajes.

Si bien este mecanismo brinda un nivel básico de seguridad, tiene como desventaja que la información de usuario y clave se transmite en texto plano, permitiendo que puedan obtenerse los datos de las credenciales por parte de dispositivos externos si se tuviese la posibilidad de capturar tramas de la comunicación.

En la Figura 2 se muestran las tramas capturadas durante el proceso de evaluación realizado, donde se visualiza que tanto los datos de usuario y clave como los tópicos y la información misma están en texto plano y son fácilmente reconocibles.

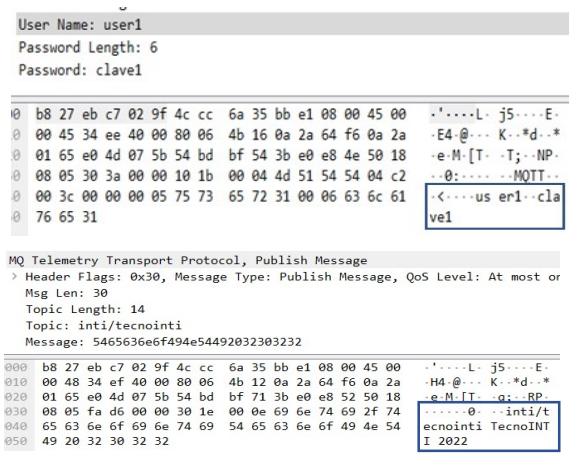

Figura 2 – Tramas de comunicación capturadas

Un segundo nivel de protección fue la incorporación en el broker de ACLs (listas de control de acceso). En ellas se definen los usuarios que pueden acceder y se especifican los tópicos permitidos. Se define también el tipo de acceso que tendrán: lectura, escritura o ambos (equivale a suscribir, publicar o los dos). Al igual que en el caso anterior la información se transmite en texto plano.

El tercer método implementado fue la transmisión cifrada de la información mediante el uso del protocolo TLS/SSL. De esta manera, se establece un canal seguro de comunicación encriptada entre cliente y broker. Para lograrlo se generaron los archivos de claves y certificados para los clientes y el broker, los cuales son intercambiados en el envío y recepción de datos con MQTT. Estos certificados deben ser validados con una Autoridad de Certificación (CA). En la implementación se utilizó el software OpenSSL para la generación de certificados y el mismo servidor Raspberry Pi cumplió la función de CA. [2]

En la Figura 3 se observa la captura de trama de dicha comunicación donde no puede identificarse ningún segmento de la información transmitida ya que la misma se encuentra encriptada.

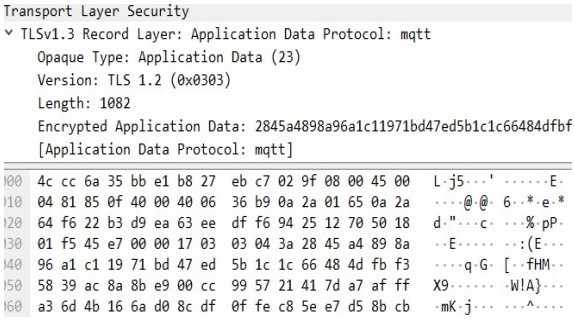

Figura 3 – Trama de comunicación con TLS/SSL

RESULTADOS

Se lograron implementar en los dispositivos que formaron parte de la evaluación los mecanismos de seguridad descriptos y se realizaron intercambios de información entre los mismos, de acuerdo a los niveles de seguridad previstos.

DISCUSIÓN Y CONCLUSIONES

Dado el constante crecimiento de las conexiones de redes OT privadas a las redes públicas, es importante establecer mecanismos que brinden seguridad frente a posibles ciberataques. MQTT ofrece medios de seguridad adecuados para lograrlo.

La implementación de las medidas “ACLs” y “usuario+clave” presenta la vulnerabilidad mencionada de la visibilidad de la información transmitida. Sin embargo, con estos mecanismos se obtiene cierto grado de seguridad en las comunicaciones sin generar carga significativa en el procesamiento en los clientes ni en el uso de ancho de banda.

Con el uso del protocolo TLS/SSL, y agregando los métodos de autenticación y autorización antes descriptos (“usuario+clave” y “ACLs”), se logra una comunicación segura y confiable entre el broker y los clientes de las redes OT, disminuyendo significativamente la posibilidad de sufrir ciberataques.

La elección de estos mecanismos deberá realizarse según las necesidades planteadas y maximizando el nivel de seguridad en función de los recursos de los dispositivos y la infraestructura de red disponible.

REFERENCIAS BIBLIOGRÁFICAS

[1] “Crytpography and SSL/TLS Toolkit”. https://www.openssl.org.
[2] “Mosquitto Documentation”, https://mosquitto.org/documentation.