Propuesta de Proyecto de Investigación
Maestría en Ciencias y Tecnologías de la Información

<2, diciembre, 2022>

1. **Nombre del proyecto "Integración de un mecanismo de autenticación en un ambiente MQTT para dispositivos de gama baja"**

2. **Responsable(s)**
   Luis Martín Rojas Cárdenas, DIE UAM, T314, lmrc@xanum.uam.mx

3. **Área(s) de conocimiento relacionada(s) con el proyecto**
   Redes de computadoras

4. **Descripción del proyecto**
   - Contexto
     El concepto de Internet de las cosas (IoT) es una de las tecnologías más prometedoras de los últimos años, se prevé que para el 2023 habrá 29,300 millones de dispositivos electrónicos conectados a Internet en el mundo y la mitad de ellos serán dispositivos IoT. Para que los dispositivos puedan comunicarse, se requiere de un protocolo estandarizado. En la actualidad, existen numerosos candidatos para volverse el protocolo estándar para el IoT, pero uno en particular ha ganado terreno en la comunidad: el protocolo MQ Telemetry Transport (MQTT). Una de las principales preocupaciones al utilizar MQTT en las redes de IoT es la seguridad. MQTT fue concebido originalmente para su uso en redes cerradas por lo que la seguridad no fue una de las consideraciones clave durante su diseño. Existen diversos problemas cuando se habla de seguridad: autenticación, integridad, confidencialidad, etc. En este trabajo se aborda en particular el problema de la autenticación, es decir, cómo tener la certeza de quien accede al dispositivo es quien dice ser.
   - Motivación
     Los sistemas embebidos con capacidades de comunicación que se integran al Internet son cada vez más numerosos. Sin importar el tipo de aplicación para la cual estén destinados o el nivel de rango e importancia del sistema, la tecnología de los IoT debería contar con sistemas de contención destinados a anular todo tipo de ataque proveniente de la red. En efecto, por el simple hecho de estar conectados, estos sistemas están a merced de cualquier tipo de ente malicioso con intenciones diversas pero en todo caso ilegitimas, poco éticas y con consecuencias que pueden ser irreparables. La cantidad de trabajos que ofrecen soluciones a los problemas de seguridad en el terreno de los IoT, si bien numerosos, aun no son definitivos. Un primer análisis del estado del conocimiento muestra que los trabajos para robustecer la seguridad de los IoT enfocan sus esfuerzos en los sistemas embebidos con sofisticados recursos de cómputo.

     En efecto, en la literatura, uno de los principales obstáculos que se mencionan para no integrar mecanismos robustos de autenticación en los sistemas IoT es su baja capacidad de cómputo. Los estudios se centran en dispositivos capaces de implementar complejos algoritmos de cifrado o en el uso de canales alternativos de comunicación para la autenticación, dejando de lado los dispositivos de gama baja, incapaces de realizar su función e implementar estas soluciones al mismo tiempo debido a los reducidos recursos con los que cuenta, entre otros, un bajo poder de cálculo y una memoria reducida. Este trabajo busca proveer un mecanismo de autenticación confiable y funcional para estos dispositivos.
   - Aporte esperado al área de conocimiento
     - Realizar un análisis del estado del conocimiento sobre los métodos de autenticación para el tipo de dispositivos objeto de este estudio.

- Proponer un método de autenticación dimensionado a las capacidades de dispositivos de gama baja sin reducir considerablemente la confiabilidad.

5. Objetivos

- Objetivo general
  Diseñar un sistema de autenticación para redes IoT basadas en el protocolo MQTT que sea funcional en dispositivos con bajo poder de cómputo.
- Objetivos particulares
  - Evaluar las alternativas tecnológicas que permitan desarrollar el sistema de autenticación propuesto que cumpla con los requerimientos definidos.
  - Diseñar e implementar una propuesta de mecanismo de autenticación que pueda cohabitar con el protocolo MQTT.
  - Evaluar y comunicar los resultados.

6. Metodología

Las siguientes actividades se desarrollarán en el marco de este trabajo:

a) Estudiar las características de los sistemas de autenticación actualmente propuestos para el IoT.
b) Seleccionar aquellos potencialmente adaptables a dispositivos de gama baja.
c) Identificar las razones por las cuales se ha preferido relegar los dispositivos de gama baja del uso de métodos de autenticación.
d) Adaptar o diseñar un método de autenticación que pueda ser utilizado en los dispositivos de gama baja así como determinar cuales los requerimientos mínimos para que este pueda operar en tales dispositivos.
e) Comparar el método diseñado en la actividad (d) con las seleccionadas en la actividad (b).
f) Reportar los resultados obtenidos en una ICR.

7. Calendarización de actividades

El proyecto se desarrollará considerando el siguiente programa de actividades,

Primer trimestre.
- Planteamiento del problema
- Revisión del Estado del Conocimiento
- Documentación

Segundo trimestre.
- Diseño de la propuesta de solución
- Desarrollo de la solución
- Documentación

Tercer trimestre.
- Desarrollo de la solución
- Primera versión de la idónea comunicación de resultados (ICR)

Cuarto Trimestre.
- Revisión de la idónea comunicación de resultados (ICR)
- Ajustes al ICR
- Preparación y presentación del examen de grado

8. Infraestructura necesaria y disponible

- Un laboratorio en donde pueda montar una maqueta MQTT.
- Contar con diversos dispositivos IoT de diferentes características.

- Un acceso al Internet y una red local de tipo WIFI e Ethernet

9. Lugar de realización

Los recursos y el espacio de trabajo será el laboratorio TAMDI, sala T329bis.

10. Entregables

- Memoria en extenso en congreso nacional o internacional.
- ICR.

11. Referencias bibliográficas básicas

[1] B.K. Tripathy and J. Anuradha, Internet of Things(IoT): Technologies, Applications, Challenges and Solutions, CRC Press, 2018.

[2] Dan Dinculeană and Xiaochun Cheng, Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices, MDPI, Journal of Applied Sciences, 2019.

[3] Ismail Butun, Patrik Österberg and Houbing Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 22, NO. 1, FIRST QUARTER 2020.

[4] Ahmed J. Hintaw, Selvakumar Manickam, Mohammed Faiz Aboalmaaly & Shankar Karuppayah (2021): MQTT Vulnerabilities, Attack Vectors and Solutions in the Internet of Things (IoT), IETE Journal of Research, DOI: 10.1080/03772063.2021.1912651

[5] D. Dinculeană and X. Cheng, "Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices," Applied Sciences, vol. 9, no. 5, p. 848, Feb. 2019, doi: 10.3390/app9050848.

[6] S. N. Firdous, Z. Baig, C. Valli and A. Ibrahim, "Modelling and Evaluation of Malicious Attacks against the IoT MQTT Protocol," 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017, pp. 748-755, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.115.

[7] I. Butun, P. Österberg and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures," in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 616-644, Firstquarter 2020, doi: 10.1109/COMST.2019.2953364.

[8] Ordóñez-Camacho, Diego. "Reduciendo La Brecha De Seguridad Del Iot Con Una Arquitectura De Microservicios Basada En Tls Y Oauth2. (Spanish)." Ingenius, Revista Ciencia y Tecnología, no. 25, Jan. 2021, pp. 94–103. EBSCOhost, https://doi.uam.elogim.com/10.17163/ings.n25.2021.09.

[9] Buccafurri, Francesco, Vincenzo De Angelis, and Roberto Nardone. "Securing MQTT by Blockchain-Based OTP Authentication." Sensors (Basel, Switzerland) 20, no. 7 (April 3, 2020). doi:10.3390/s20072002.