Definición Broker Comunicaciones desde una perspectiva de Confianza

Enfoque:

Gestor de Confianza y creación de un sistema de reputación.

Requisitos generales:

R01: Interacción segura y confiable

Descripción: Las interacciones posibles son:

- humano - dispositivo físico;
- humano - dispositivo virtual;
- dispositivo físico - dispositivo físico;
- dispositivo virtual - dispositivo virtual;
- dispositivo físico - dispositivo virtual.

Dichas interaciones estarán protegidas haciendo uso de medidas de seguridad básicas, pero también de medidas específicas, como pueden las asociadas con el control de acceso (p. ej., guiado por los principios de identidad soberana establecidas y gestionado a través de una blockchain), o los mecanismos de confianza para crear interfaces onfiables.

R02: Gestión de confianza

Descripción: Un sistema o modelo de gestión de confianza entre los diferentes componentes y entidades que interactúan, integran o conforman la plataforma deberá ser proporcionada.
En este caso, se tendrá en cuenta los mecanismos actuales propuestos en la literatura, a fin de buscar la forma de medir el nivel de confianza entre elementos e interacciones con la plataforma. Una de las estrategias puede ser, por ejemplo, el uso de los certificados digitales o el diseño de un sistema específico capaz de calcular el nivel de reputación de cada componente. Por ejemplo, si un dispositivo/usuario no tuvo el comportamiento esperado dentro/a través de la plataforma, el valor de su reputación se verá afectada, haciendo que el resto de los componentes disminuyan la confianza puesta en él.
Esto último, puede, incluso, beneficiar los procesos de mantenimiento de los módulos de la plataforma (ej. los mecanismos de detección de intrusiones o de respuesta), y determinar el grado de fiabilidad y precisión de los módulos de seguridad (ej. el de detección temprana, el de respuesta).

Gestor de confianza

El detección de anomalias es como si fuese una “caja negra”, nos vamos a centar en el gestor de confianza y en los datos que nos proporciona el detección de anomalias, lo que tenemos que proporcionales y otros datos importantes para poder computar el nivel de confianza.

Relacciones y datos intercambiados entre bloques

• Detección de anomalías -> Gestor de confianza

- ID
- Gravedad de la anomalía detectada

• Gestor de confianza -> Detección de anomalías

- ID
- Nivel de confianza

Segune este esquema se deberá crear un modelo de confianza según la anomalia detectada. Proporcionar un modelo basado en el paper [1] donde según la anomalia detectada se hará un nuevo calculo de la confianza/reputación del dispositivo y se proporcionará un nuevo nivel de confianza al sistema de Detección de anomalías. Una posibilidad puede ser simular dichos modulos con Docker, Raspberry Pi y/o Codigo Java.

Además, se tiene que gestionar dicha comunicación a través de un protocolo MQTT [2] para transmitir los datos de manera confiable y segura.

References:

[1] Ferraris, D., Fernandez-Gago, C., Daniel, J., & Lopez, J. (2019, January). A segregated architecture for a trust-based network of internet of things. In 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC) (pp. 1-6). IEEE.

[2] La Marra, A., Martinelli, F., Mori, P., Rizos, A., & Saracino, A. (2017). Improving MQTT by inclusion of usage control. In Security, Privacy, and Anonymity in Computation, Communication, and Storage: 10th International Conference, SpaCCS 2017, Guangzhou, China, December 12-15, 2017, Proceedings 10 (pp. 545-560). Springer International Publishing.