1. Describa en qué consisten los siguientes ataques a la seguridad en IoT:

- Node capture attack:
  El node capture attack se da normalmente en redes de sensores inalámbricos donde el intruso realiza varias operaciones comprometiendo la red. El atacante remueve varios nodos sensores y los reinstala para realizar varios ataques. Estos nodos reinstalados son usados para modificar la información en el canal de comunicación de la red de sensores.
- Malicious code injection attack:
  Ocurre cuando el atacante realiza una validación maliciosa en la entrada del software inyectado código malicioso. Este código es interpretado por la aplicación y cambia el sentido del programa.
- Sleep deprivation attack:
  Es cuando un nodo malicioso realiza requests de manera que mantenga a las victimas lo necesario para que sigan despierto. Esto para que el nodo victima se quede despierto, sin que realice operaciones que requieran gran cantidad de energía
- DoS:
  Uno de los ataques más comunes de Dos es el jamming donde un nodo malicioso bloquea legítimamente comunicación causando una interferencia intencional en la red.
- Man in the Middle Attack (MITM):
  MITM es donde el atacante realiza acciones para poder escuchar o itervenir en el canal entre dos clientes para poder escuchar. Los delincuentes fijan estas redes usando un método llamado Address Resolution Protocol (ARP) el cual manda falsos ARP a través de un LoRaWAN
- Sybil attack:
  Este ataque usa un solo nodo para operar activades falsas simultáneamente dentro de una red peer to peer. Este tipo de ataques apunta a indeterminar la autoridad al tratar de ganar la mayor influencia de la red.

- Phishing attack:

Este tipo de ataques consta de emails, mensajes, etc conteniendo contenido malicioso o intentando persuadir al usuario a hacer click a un link y sin saber compartir la información personal o credenciales con el atacante.

2. Escriba un ensayo de una cuartilla de entre 200 y 250 palabras donde analice por qué es importante la seguridad en IoT y qué efectos tiene el no implementar medidas adecuadas de seguridad. Describa un ejemplo real de un ataque a la seguridad o un caso hipotético bien documentado.

La seguridad en IoT es importante debido a que actualmente hay muchos dispositivos que conectados a la red que se maneja información muy sensible donde cualquier ataque puede costar mucho dinero inclusive poner vidas en riesgo.

Un ejemplo de ataque es en plantío donde un WSN un atacante toma el nodo Gateway por medio de node capture attack, ya que este nodo al estar conectado directamente con internet cuenta con una ip y el atacante logra entrar encontrando una falla de seguridad, el atacante al tener el nodo Gateway puede realizar operaciones de mandar información tanto a donde se almacenan los datos de toda la WSN y también para que los actuadores que procesan la información de toda la red vean los datos que el atacante está metiendo de manera que estos activen a los sensores actuadores y empiecen a regar todos los plantíos o hace otra acción y si no se llega a mitigar el ataque todos los plantíos pueden llegar a arruinar muchos lotes de plantíos ocasionando perdidas millonarias para la empresa. El atacante puede optar por borrar los datos que van llegando a este nodo sean incorrectos y cuando estos datos en un futuro quieran ser analizados o procesados toda la veracidad de estos datos será incorrecta tanto como los resultados a los que se lleguen con los análisis debido a que no serán los datos reales obtenidos de los sensores sino datos que el atacante introdujo.

Referencias:

https://www.sciencedirect.com/science/article/pii/S2666285X2100073X

https://www.akana.com/blog/malicious-code-injection

https://journals.sagepub.com/doi/10.1080/15501320600642718

https://www.sciencedirect.com/topics/engineering/denial-of-service-attack

https://scholarworks.montana.edu/xmlui/bitstream/handle/1/9021/jamming.pdf

https://arxiv.org/pdf/2308.02479.pdf

https://www.imperva.com/learn/application-security/sybil-attack/