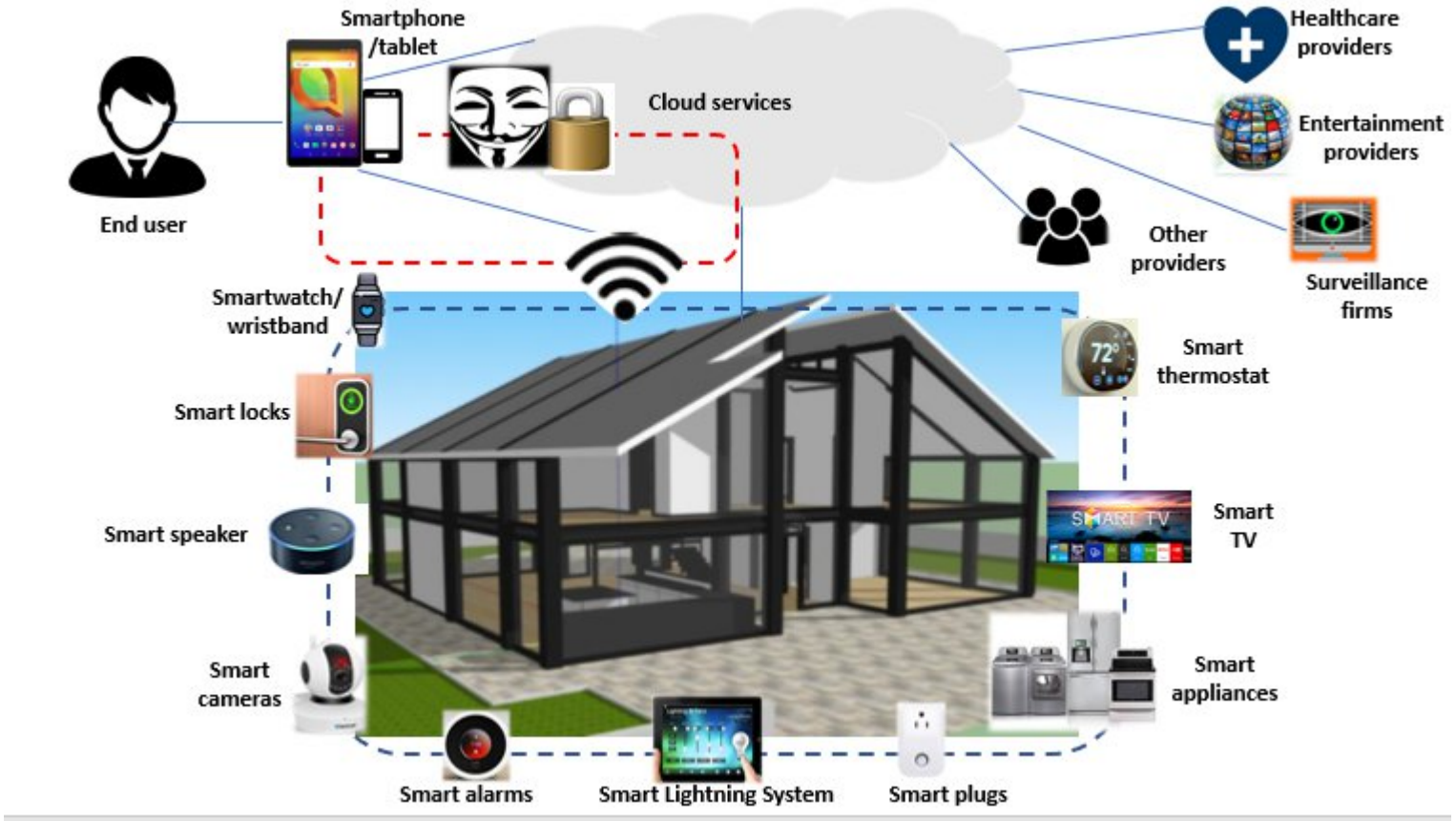
Seguridad en IoT



Seguridad en IoT

Cualquier dispositivo inteligente puede servir como punto de entrada para que los ciberdelincuentes accedan a la red.

La interacción y la educación del usuario es un desafío.

Los consumidores desconocen la importancia de actualizar el software y firmware a la última versión disponible.

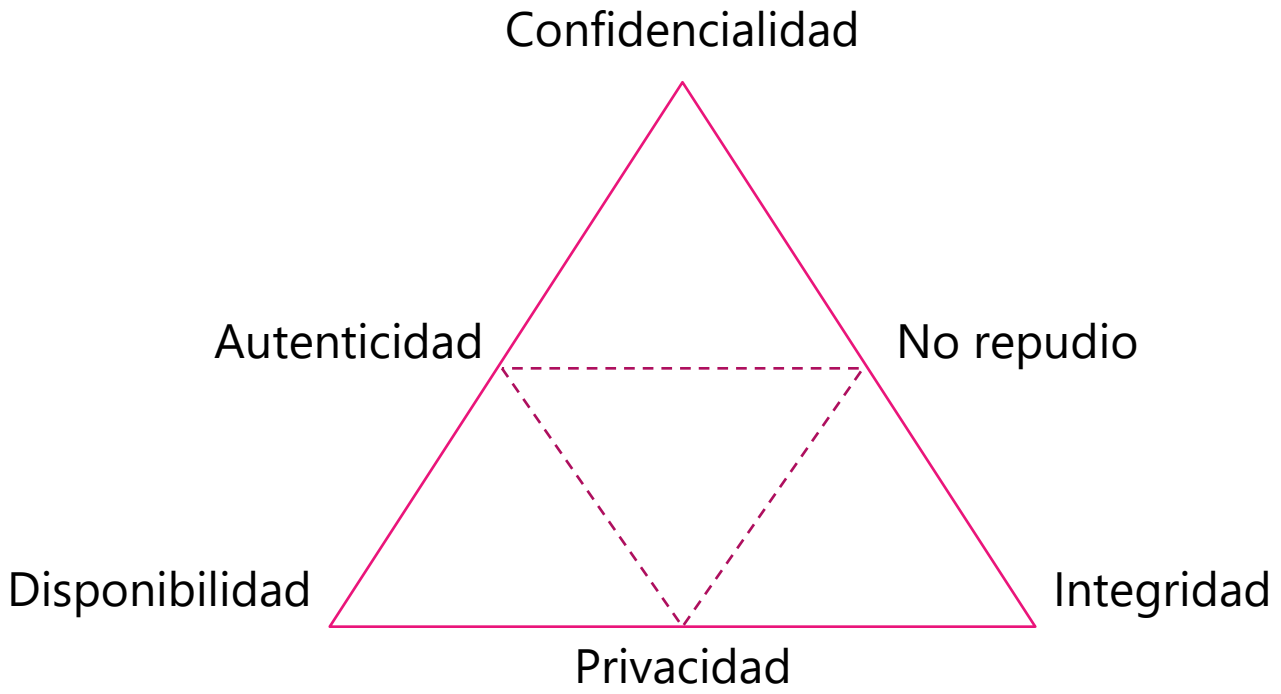
Propiedades de seguridad

Confidencialidad

Privacidad

Confianza

Requerimientos de seguridad en IoT



Ataques comunes en dispositivos IoT

Mejores prácticas

Usuarios

- SW y FW actualizado
- Uso de contraseñas seguras / Uso de manejadores de contraseñas
- Habilitar autenticación multifactor

Negocios

- Desarrollar e implementar una política de dispositivos IoT
- Compilación y mantenimiento de una lista maestra de todos los dispositivos IoT
- Monitoreo de todos los dispositivos de red
- Cifrar todos los datos

Taller

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

    a) Node capture attack.
    b) Malicious code injection attack.
    c) Sleep deprivation attack.
    d) DoS.
    e) Man in the Middle Attack (MITM).
    f) Sybil attack.
    g) Phishing attack.

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.