[CSIOT] Tema 3: Seguridad de dispositivos IIoT: Hardware, Firmware y Middleware

- La loT Security Foundation (IoTSF) establece directrices básicas y un enfoque para autocertificación
 - Proporciona una guia de buenas prácticas y clasifica los dispositivos en sensores, actuadores y gateways
 - Establece áreas que se deben considerar:
 - Clasificación de los datos
 - Seguridad física
 - Arraque seguro de los dispositivos
 - Sistema operativo seguro
 - Seguridad de las aplicaciones
 - Getión de credenciales
 - Cifrado
 - Conexión de red
 - Securización de las actualizaciones de software
 - Registro
 - Política de actualización de sfotware
 - Evaluar el proceso de arrangue seguro
 - Imagenes y firmas de las actualizaciones de software
 - Ataques de canal lateral
- La Platform Security Architecture (PAS) se centra en sistemas basados en MCU y MPU. Esta diseñado para mejorar la seguridad de los dispositivos IoT.
 - Los dispositivos:
 - Tiene que ser identificables de manera única
 - Soportan un ciclo de vida de seguridad
 - Son verificables de forma segura
 - garantizan que solo se puede ejecutar software autorizado
 - soportan actualizaciones seguras
 - soportan aislamiento
 - soportan interacción sobre las fronteras de aislamiento
 - soportan un conjunto minimo de servicios de confianza y operaciones criptofráficas.
- Security Evaluation Standard for IoT Platforms (SESIP)
- Internet of Secure Things (IoXt)

Panorama de amenazas y enfoque sistemático

Modelado de amenazas

Proceso de:

- 1. Comprender un sistema
- 2. Identificar amenazas a este
- 3. Clasificar las amenazas en función a impacto y probabilidad

Last update: 2025/05/22 21:05

En el caso del modelo de microsoft este proceso es algo diferente:

- 1. Identificar activos
- 2. Describir arquitectura
- 3. Descomponer la aplicación
- 4. Identificar amenazas
- 5. Documentar amenazas
- 6. Clasificar amenazas (STRIDE):
 - 1. Spoofing: El atacante puede acceder con una identidad falsa
 - 2. Tampering: El atacante puede modificar los datos que fluyen a través de la apliación
 - 3. Repudiation: Un atacante puede bloquear una acción
 - 4. Information Disclosure: Un atacante puede acceder a datos privados o perjudiciales
 - 5. Denial of Service: Un atacante puede producir fallos o reducir la disponibilidad del sistema
 - 6. Elevation of priviledge: Un atacante puede tomar la identidad de un usuario privilegiado.

From:

http://knoppia.net/ - Knoppia

Permanent link:

http://knoppia.net/doku.php?id=master_cs:csiot:tm3&rev=1747947916

Last update: 2025/05/22 21:05

http://knoppia.net/ Printed on 2025/11/29 09:38