Rol de la seguridad en el desarrollo de IoT

Los dispositivos IoT tienen recursos limitados

Diseñados para consumir poca energía

A pesar de lo anterior, están diseñados para proporcionar toda la funcionalidad requerida a un costo razonable

RESULTADO

La seguridad es una idea de último momento, a menudo colocada al final de la lista de prioridades en el ciclo de vida del desarrollo.

Seguridad en IoT

Los vectores de ataque de IoT pueden apuntar a dispositivos, gateways y wearables y pueden aprovechar contraseñas débiles, falta de cifrado, puertas traseras, etc.

La amplia variedad de sistemas operativos específicos de IoT, versiones de firmware y configuraciones personalizadas dificulta el desarrollo de soluciones generales de seguridad de IoT.

Las soluciones de seguridad de IoT deben ser escalables para poder aplicarse a un número cada vez mayor de dispositivos IoT diferentes.

Ataques y amenazas a la seguridad en IoT

Amenaza	Procedimiento de ataque	Requerimiento de seguridad	Ejemplos
Ataques físicos	Alterar el hardware y otros componentes.	Resistencia a manipulaciones	Reconstrucción del diseño, microsondeo.
Ataques en el entorno	El atacante puede descubrir la llave de cifrado del dispositivo por medio de textos cifrados.	Mecanismo de cifrado seguro	Timing attack, side-channel attack, fault analysis attack
Ataques de criptoanálisis	Uso de un texto cifrado para romper el mecanismo de cifrado.	Mecanismo de cifrado seguro	Known-plaintext attack, chosen plaintext attack
Ataques en el software	Explotar vulnerabilidades en el sistema durante su propia interfaz de comunicación e inyectar códigos maliciosos.	Actualización apropiada de antivirus	Caballos de troya, virus

Taxonomía de ataques según las fases del proceso de IoT

Fase	Ataque/Amenaza	Descripción
Percepción de datos: se pueden utilizar varios tipos de recolectores de datos. El servicio puede ser un cuerpo estático (sensores corporales o etiquetas RFID) o dinámico.	Fuga o violación de datos, pérdida de datos, autenticación de datos.	La fuga de datos puede ser interna o externa, intencional o no, e involucrar hardware o software.
Almacenamiento. Si el dispositivo tiene su propia memoria local, se pueden almacenar datos. En el caso de dispositivos sin estado, los datos se pueden almacenar en la nube.	Ataque a la Disponibilidad, Control de Acceso, Integridad, Denegación de Servicio, Suplantación.	La disponibilidad es una de las principales preocupaciones de seguridad. DDoS es una condición de sobrecarga causada por una gran cantidad de atacantes distribuidos

Taxonomía de ataques según las fases del proceso de IoT

Fase	Ataque/Amenaza	Descripción
Procesamiento inteligente	Ataque a la autenticación	Una solución de IoT que proporciona análisis de datos y servicios inteligentes en tiempo real.
Transmisión de datos	Seguridad del canal, secuestro de sesión. Protocolos de enrutamiento, flooding.	Amenazas en la transmisión, como interrupción, bloqueo, manipulación de datos, falsificación, etc.

Confianza, confidencialidad de datos y privacidad en IoT

La confianza y la seguridad se basan en tokens o credenciales, proporcionados por una infraestructura de gestión de confianza, que están integrados y potencialmente compartidos entre dispositivos.

Estos tokens pueden ser claves simétricas o certificados digitales.

Ataques externos ✓

Ataques internos ✗

Ejemplo

Ejemplo

La bomba de insulina debe poder validar que realmente se conecta a un glucómetro confiable y no a un dispositivo malicioso

La prueba de autorización proporciona seguridad de que un par tiene la autoridad para:

- Comunicarse con otro par
- Realizar una determinada acción

Privacidad

La privacidad implica la seguridad de la información personal, así como la capacidad de controlar lo que sucede con esta información.

Se puede recopilar mucha información privada de los dispositivos inteligentes.

En muchos casos, los datos se recopilan de forma pasiva y, debido a ello, algunas violaciones de la privacidad pueden pasar desapercibidas durante mucho tiempo.

Privacidad

Los usuarios finales creen que son dueños de todos los datos.

Los proveedores de servicios creen que son propietarios de los datos, al igual que los proveedores de aplicaciones.

Los fabricantes de los dispositivos creen que poseen, o al menos tienen derechos de acceso, a los datos generados por sus dispositivos.

Ejemplo

Combinaciones aparentemente benignas de flujos de datos de IoT procedentes de diversas fuentes pueden poner en peligro la privacidad.