Gaytan Herrera Belen
Rojas Jimenez Claudia Alin

Modelo de amenazas

Assets:

- Documentos originales
- Archivos cifrados almacenados o transmitidos.
- Claves privadas de los usuarios.
- Claves simétricas generadas por archivo.
- Firmas digitales.
- Copias de seguridad de claves.
- Contraseñas utilizadas para proteger claves privadas.

Attackers:

- **Atacante Pasivo**
  - Puede interceptar comunicaciones (sniffing).
  - Puede observar archivos almacenados.
  - No puede modificar datos.

- **Atacante Activo**
  - Puede modificar archivos cifrados.
  - Puede intentar reemplazar claves públicas.
  - Puede eliminar o alterar copias de seguridad.
  - Puede intentar ataques de ingeniería social.
  - Puede intentar ataques de fuerza bruta contra contraseñas.

Mecanismos:

- Cifrado
- Administración de Llaves públicas y privadas
- Mecanismos de autenticación
- Copia de seguridad
- Verificación de integridad