
Grupo de Seguridad Informática

# Fundamentos de la Seguridad Informática

## Modelado de Amenazas

# Modelado de Amenazas

- *Threat Modeling o también Análisis de riesgo de Arquitectura*
- Ayuda a los diseñadores de sistemas acerca de las amenazas de seguridad a las que se enfrentan sus sistemas
- Permite desarrollar estrategias de mitigación para vulnerabilidades potenciales

# ¿Qué queremos resolver con TM?

Las técnicas de TM usan los cuatro pasos siguientes:

1) ¿Qué estamos construyendo?
2) ¿Qué puede salir mal?
3) ¿Qué vamos a hacer al respecto?
4) ¿Hicimos un buen trabajo?

# ¿Qué estamos construyendo?

- Ejemplos de técnicas usadas:
  - Diagramas de arquitectura
  - Diagramas de flujo
  - Clasificación de datos
- Juntar personas en diferentes roles con conocimiento técnico y en riesgos para acordar el framework a ser usado en el ejercicio de TM

# ¿Qué puede salir mal?

- Esta es una actividad de “investigación” en la cual se quieren encontrar la principales amenazas que aplican a nuestra aplicación
- Diversas formas:
  - Braninstorming
  - Usando estructuras que nos ayuden
    - STRIDE, Kill chains, CAPEC, etc

# ¿Qué vamos a hacer al respecto?

- Esta fase transforma lo encontrado en acciones específicas
  - Cambio en diagramas
  - Creación de bugs
  - Nuevos requerimientos
  - Nuevas *user stories* al backlog

# ¿Hicimos un buen trabajo?

- Finalmente, se hace una actividad retrospectiva sobre el trabajo realizado para verificar calidad, que sea viable, el progreso y/o la planificación

# El proceso

- Puede ser informal usando Kanban o Post-its en la pared
- El esfuerzo, trabajo, y tiempos invertidos en TM se relacionan al proceso de ingeniería que se está usando
- Puede ser usada independiente del proceso de desarrollo (Agile, Waterfall, etc)

# Técnicas

- Cyber Kill Chain
- MITRE ATT&CK
- STRIDE
- Common Attack Pattern Enumeration and Classification (CAPEC™)
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) (CMU)

# Cyber Kill Chain

- Acceso Inicial
- Ejecución
- Persistencia
- Escalada de Privilegios
- Evasión de defensas
- Acceso a credenciales
- Descubrimiento
- Movimiento lateral
- Recolección
- Command and control
- Exfiltración
- Impacto

# STRIDE

- Usando el Proceso de Modelado de Amenaza de Microsoft (STRIDE)
- Ejecutando modelado de riesgo de amenazas
  - Flujo del Modelo de Amenaza
  - Identificar Objetivos de Seguridad
  - Visión General de la Aplicación
  - Descomponer la aplicación
  - Documentar las amenazas conocidas

# STRIDE

- Categorías:
  - Spoofing of user identity (Impersonar)
  - Tampering (Falsificación, alteración)
  - Repudiation (Repudio)
  - Information disclosure (privacy breach or Data leak) (filtrado de información)
  - Denial of Service (DoS, Denegación de servicio)
  - Elevation of privilege (Elevación de privilegios)

# Impersonar

- Amenaza que apunta a acceder ilegalmente a las credenciales de otro usuario, como nombre de usuario y clave
- Control asociado: autenticación
- Mitigación: autenticación apropiada, proteger datos secretos, no guardar secretos

# Falsificar

- Amenaza que apunta a cambiar/modificar datos persistentes y la alteración de data en tránsito entre dos computadores
- Control asociado: Integridad
- Mitigación: autenticación apropiada, hashes, MACs, firmas digitales, protocolos resistentes

# Repudio

- Apunta a realizar operaciones ilegales en un sistema que no tiene la habilidad de tracear las operaciones prohibidas
- Control asociado: no repudio
- Mitigación: firmas digitales, timestamps, caminos de auditoría

# Filtrado de información

- Leer un archivo o recurso del cual no se tiene acceso, o leer datos en tránsito
- Control asociado: confidencialidad
- Mitigación: autorización, protocolos de privacidad mejorada, encriptación, proteger secretos

# Denegación de servicio

- Enfocada a denegar el acceso a usuarios válidos, como por ejemplo tener que un servicio web
- Control asociado: disponibilidad
- Mitigación: filtrado, autenticación y autorización apropiadas, regulación, QoS

# Elevación de Privilegios

- Obtener acceso privilegiado a recursos para ganar acceso no autorizado a información o comprometer un sistema
- Control asociado: autorización
- Mitigación: ejecutar con mínimo privilegio

# Controles de seguridad

- Deben identificarse para prevenir el impacto de las amenazas
- Al realizar la revisión de código (y testing), debe verificarse que están en el lugar apropiado
- Y que son invocados en los lugares que corresponde

# Control: autenticación

- Asegurar todas las conexiones internas y externas (usuarios y entidades)
- Asegurar que las credenciales de autenticación no atraviesen los cables en texto plano
- Asegurar que puertas traseras de desarrollo/debug no estén presentes en el código de producción

# Control: autorización

- Asegurar que la aplicación ha definido claramente los tipos de usuarios y los derechos de estos usuarios
- Asegurar que la autorización se verifica en cada pedido
- Asegurar que la actidud de mínimo privilegio está en operación

# Control: Validación de entradas/Datos

- Asegurar que existe un mecanismo de validación
- Asegurar que todos los datos de un formulario/pantalla son validados
- Regla de Oro: *toda entrada externa, no importa lo que sea, es examinada y validada.*

# Control: manejo de errores/filtración de información

- Asegurar que las excepciones y otras condiciones de error se manejan de forma adecuada
- Examinar si la aplicación audita las acciones tomadas en nombre del cliente
- Tanto autenticación exitosa como no son registradas

# Control: criptografía

- Asegurar que no se transmiten datos sensibles en claro, tanto interna como externamente
- Asegurar que se implementen métodos criptográficos conocidos

# DREAD:el modelo de clasificación de riesgos

- Factores de riesgo técnico: *Damage* (Daño) y *Affected Users* (usuarios afectados)
- Facilidad de explotación: Reproducibilidad, explotabilidad, discoverability
- Del 1 al 10

# Referencias

- OWASP Threat Dragon https://threatdragon.org/
- STRIDE, Microsoft https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx
- CAPEC, https://capec.mitre.org