DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

1.5. Introducción – Amenazas y su modelado

Fundamentos de ciberseguridad

Profesor

Juan Ignacio Iturbe A.

Objetivos de aprendizaje

- OA9: Conocer algunas de las taxonomías de ataques y amenazas existentes.
- OA10: Reconocer amenazas sobre sistemas en diseño y producción.
- OA11: Crear modelos de amenazas que ayuden a la identificación de las mismas.
- OA12: Priorizar las amenazas mas importantes que afecten a un sistema.

Taxonomías de amenazas y ataques

Algunas taxonomías son:

- CAPEC: Common Attack Pattern Enumeration and Classification
- ENISA Threat Taxonomy
- LINDUNN: Amenazas a la privacidad
- Magerit: Libro II – Catalogo de elementos
- Cyber Kill Chain
- The MITRE ATT&CK Framework
- STRIDE

CAPEC: Common Attack Pattern Enumeration and Classification
(https://capec.mitre.org/)

Dominio de ataque

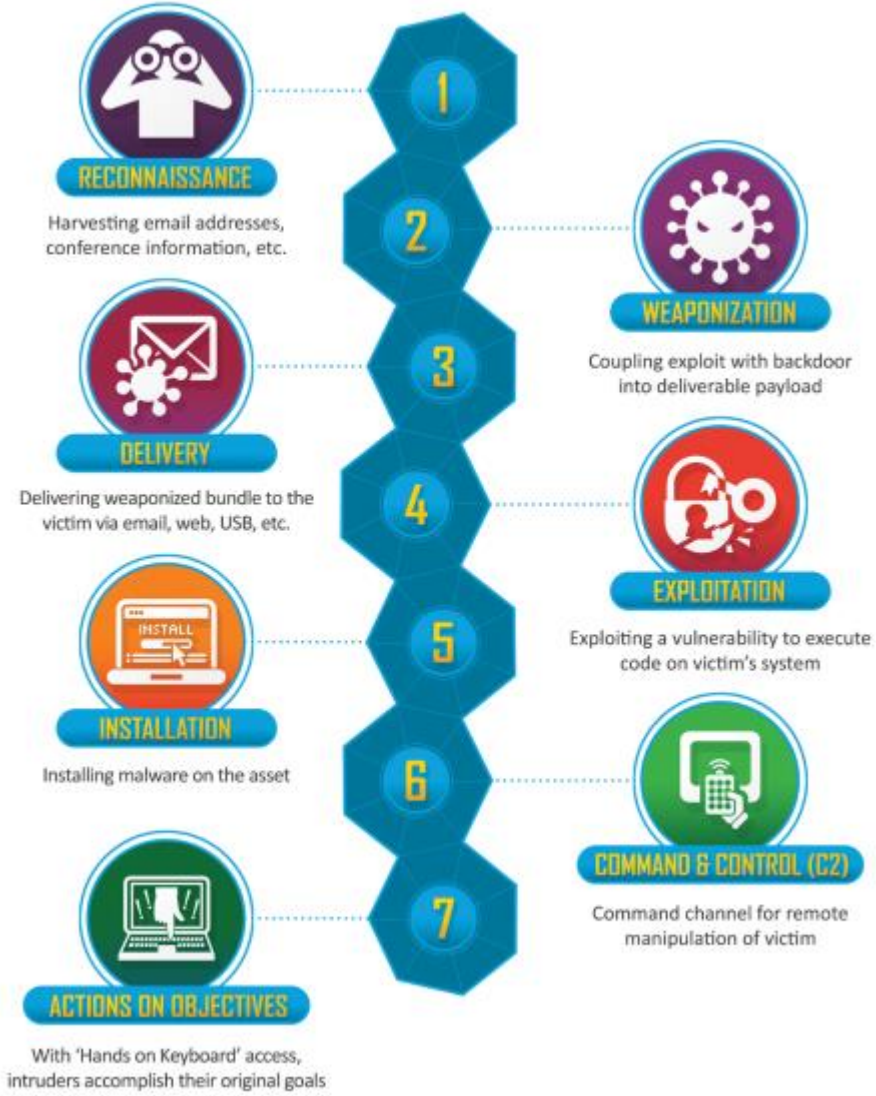
i. Software
ii. Hardware
iii. Comunicación
iv. Cadena de suministro
v. Ingeniería social
vi. Seguridad física

Mecanismo de ataque

a) Participar en interacciones engañosas
b) Abusar de la funcionalidad existente
c) Manipular estructuras de datos
d) Manipular recursos del sistema
e) Inyectar elementos inesperados
f) Emplear técnicas probabilísticas
g) Manipular tiempo y estado
h) Recopilar y analizar información
i) Control de acceso subvertido

Cyber Kill Chain

- Desarrollada el 2011 por Lockheed Martin,
- Con raíces en las operaciones militares.
- Define los pasos que un agente de amenaza debe seguir para lograr sus objetivos
- Se distinguen 7 pasos:
  1. Reconocimiento
  2. Militarización/Armamentismo
  3. Entrega
  4. Explotación
  5. Instalación
  6. Comando y control
  7. Acciones en objetivo



The MITRE ATT&CK Framework

https://attack.mitre.org/

- Marco de trabajo de tácticas adversarias, técnicas, y conocimiento común.
- Es una matriz de tácticas y técnicas utilizadas por agentes de amenazas.
- La base de conocimientos de este se utiliza como base para el desarrollo de metodologías y modelos de amenazas específicos en el sector privado, en el gobierno y en la comunidad de productos y servicios de ciberseguridad.
- Por ejemplo, una sub-técnica de “Comando y control” utiliza DNS para enviar y recibir mensajes de forma encubierta,

Agrupadas en 14 tácticas con objetivos específicos. Estas son:

1. Reconocimiento
2. Desarrollo de recursos
3. Acceso inicial
4. Ejecución
5. Persistencia
6. Escalado de privilegios
7. Evasión de defensas
8. Acceso a credenciales
9. Descubrimiento
10. Movimiento lateral
11. Colección
12. Comando y control
13. Filtración
14. Impacto

ATT&CK®

STRIDE

Tipo de amenaza	Objetivo de seguridad relacionado	Descripción
Spoofing (Suplantación)	Autenticación	Un ataque con el objetivo de obtener acceso a un sistema objetivo mediante el uso de una identidad falsificada. La suplantación de identidad se puede usar contra direcciones IP, direcciones MAC, nombres de usuario, nombres de sistemas, SSID de redes inalámbricas, direcciones de correo electrónico y muchos otros tipos de identificación lógica. Cuando un atacante falsifica su identidad como entidad válida o autorizada, a menudo puede pasar por alto los filtros y bloqueos contra el acceso no autorizado. Una vez que un ataque de suplantación de identidad ha otorgado con éxito un acceso de atacante a un sistema objetivo, se pueden iniciar ataques de abuso, robo de datos o escalada de privilegios posteriores.
Tampering (Manipulación)	Integridad	Cualquier acción que resulte en cambios no autorizados o manipulación de datos, ya sea en tránsito o en almacenamiento. La manipulación se utiliza para falsificar las comunicaciones o alterar la información estática. Tales ataques son una violación de la integridad y de la disponibilidad.
Repudiation (Repudio)	No repudiación	La capacidad de un usuario o atacante de negar haber realizado una acción o actividad. A menudo, los atacantes se involucran en ataques de repudio para mantener una negación plausible (plausible deniability) para no ser responsables de sus acciones. Los ataques de repudio también pueden dar lugar a la culpa de terceros inocentes por violaciones de seguridad.
Information disclosure (Divulgación de información)	Confidencialidad	La revelación o distribución de información privada, confidencial o controlada a entidades externas o no autorizadas. Esto podría incluir información de identidad de los clientes, información financiera o detalles de operaciones financieras. La divulgación de información puede aprovechar los errores de diseño y de implementación del sistema. Por ejemplo: no eliminar el código de depuración, dejar aplicaciones y cuentas de muestra, no eliminar las notas de programación del contenido visible del cliente (como comentarios en documentos HTML), usar campos de formulario ocultos o permitir mensajes de error demasiado detallados para mostrar a los usuarios.
Deny of Service, DoS (Denegación de servicio)	Disponibilidad	Un ataque que intenta evitar el uso autorizado de un recurso. Esto se puede hacer mediante la explotación de fallas, la sobrecarga de conexiones o la inundación del tráfico. Un ataque DoS no necesariamente resulta en la interrupción total de un recurso; en cambio, podría reducir el rendimiento o introducir latencia para obstaculizar el uso productivo de un recurso. Aunque la mayoría de los ataques DoS son temporales y duran solo mientras el atacante mantiene el ataque, hay algunos ataques DoS permanentes. Un ataque DoS permanente puede implicar la destrucción de un conjunto de datos, el reemplazo de software con alternativas maliciosas o forzar una operación flash de firmware que podría interrumpirse o que instale un firmware defectuoso. Cualquiera de estos ataques DoS generaría un sistema dañado permanentemente que no se puede restaurar a la operación normal con un simple reinicio o esperando que termine el ataque. Se requeriría una reparación completa del sistema y una restauración de respaldo para recuperarse de un ataque DoS permanente.
Elevation of privilege (Elevación de privilegios)	Autorización	un ataque en el que una cuenta de usuario limitada se transforma en una cuenta con mayores privilegios, poderes y acceso. Esto podría lograrse mediante el robo o la explotación de las credenciales de una cuenta de nivel superior, como la de un administrador o root. También podría lograrse a través de una vulnerabilidad de sistema o aplicación que otorgue poderes adicionales de manera temporal o permanente a una cuenta que de otro modo sería limitada.

STRIDE

Tipo de amenaza	Ejemplo	Ejemplos de mitigación
Spoofing (Suplantación)	Un agente externo pretendiendo ser un empleado de RRHH en un email.	Passwords, autenticación multifactor Firmas digitales
Tampering (Manipulación)	Un programa modificando los contenidos de un archivo crítico del Sistema.	Permisos/ACLs Firmas digitales
Repudiation (Repudio)	Un usuario indicando que este no recibió un pedido.	Logs de seguridad y auditoria Firmas digitales
Information disclosure (Divulgación de información)	Un analista accidentalmente revelando detalles internos de la red a externos.	Encriptación Permisos/ACLs
Deny of Service, DoS (Denegación de servicio)	Una botnet enviando grandes cantidades de solicitudes a un sitio web causando su caída.	Permisos/ACLs Captchas Filtrado de tráfico Cuotas
Elevation of privilege (Elevación de privilegios)	Un usuario saltando las restricciones locales para ganar acceso administrativo a una estación de trabajo.	Validación de entradas de usuario Permisos/ACLs

Modelado de amenazas

- Utilizamos modelos para representar realidades complejas.
- Existen demasiados agentes de amenazas haciendo muchas cosas y en muchas partes.
- Por lo tanto, nos enfocamos en probables atacantes y patrones que nos permitan mitigar una gran cantidad de diferentes ataques derrotando las técnicas que tienen en común.
- Un típico modelado de amenazas comienza identificando los agentes de amenazas que tienen probablemente nuestra organización como objetivo. Nos preguntamos:
  1. ¿Por qué alguien podría poner como objetivo nuestra organización?
  2. ¿Como podrían ellos cumplir sus objetivos?
  3. ¿Cuando y donde podrían ellos atacarnos?

1. Revisar inventario de activos.
2. Revise las taxonomías anteriores,
3. Modele su sistema y analice cuando y donde.

Modelado de amenazas

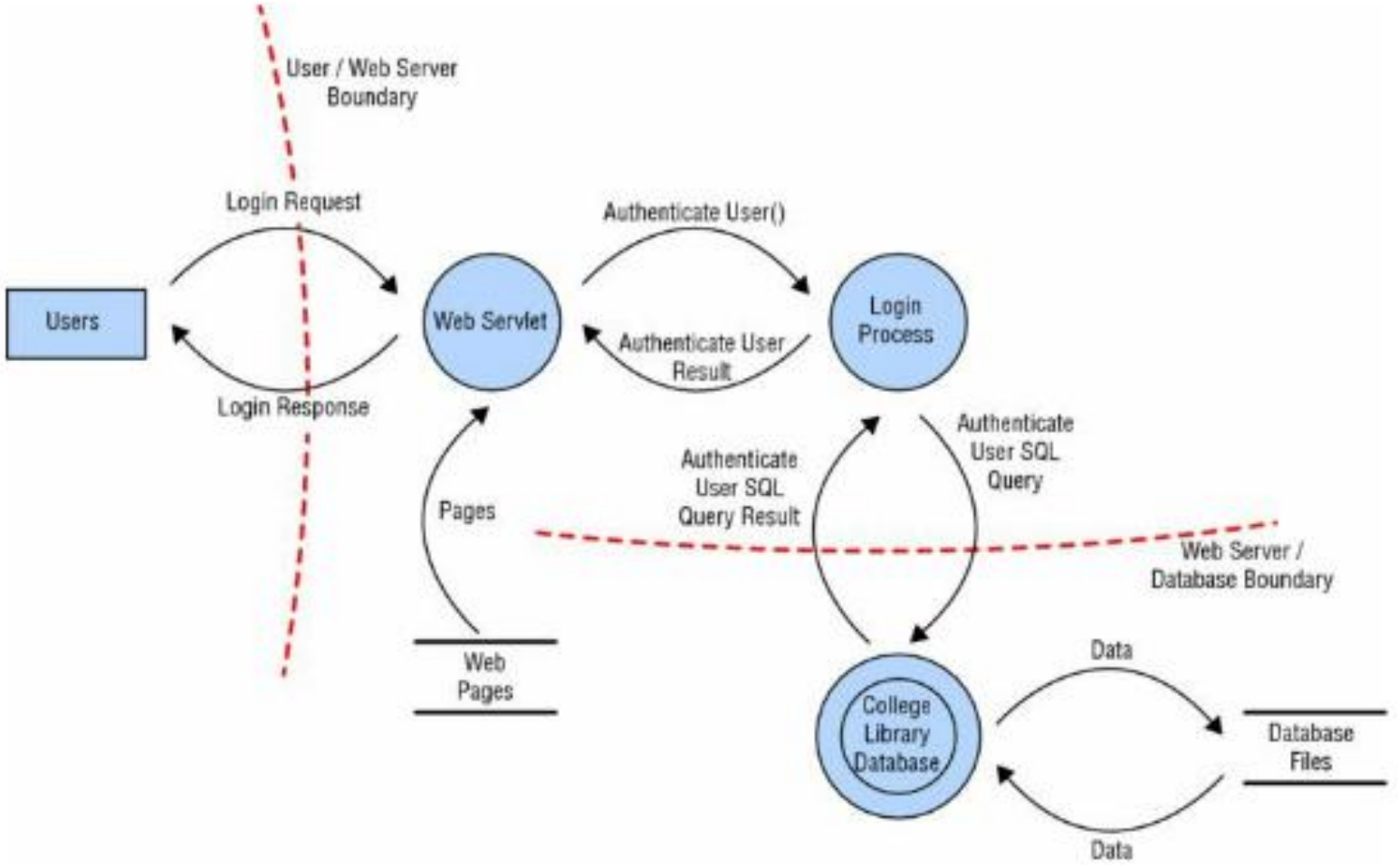
- El modelado de amenazas es el proceso de seguridad donde se identifican, categorizan y analizan las posibles amenazas.
- El modelado de amenazas se puede realizar como una medida proactiva durante el diseño y desarrollo o como una medida reactiva una vez que se ha implementado un producto.
- En cualquier caso, el proceso identifica el daño potencial, la probabilidad de ocurrencia, la prioridad de preocupación y los medios para erradicar o reducir la amenaza.
- Se intenta reducir las vulnerabilidades y reducir el impacto de cualquier vulnerabilidad que permanezca.
- Un enfoque proactivo para el modelado de amenazas tiene lugar durante las primeras etapas del desarrollo de sistemas

Identificando amenazas

- Existe una posibilidad casi infinita de amenazas, por lo que es importante utilizar un enfoque estructurado para identificar con precisión las amenazas relevantes.
- Por ejemplo, algunas organizaciones usan uno o más de los siguientes tres enfoques:
  - **Centrado en los activos:** Se requiere valorizar los activos y encontrar amenazas en los mas valiosos.
  - **Centrado en los atacantes:** Se reconoce lo que los atacantes quieren lograr. Luego, con esto se identifica y protegen los activos relevantes.
  - **Centrado en el software:** Se consideran amenazas en el proceso de desarrollo y en el software en sí.

Determinando y diagramando ataques potenciales

- El siguiente paso en el modelado de amenazas es determinar los ataques conceptuales potenciales que podrían realizarse.
- Esto se logra mediante la creación de un diagrama de los elementos involucrados en una transacción junto con indicaciones de flujo de datos y límites de confianza



Uso de DFD en el modelado de amenazas

- Los diagramas de flujo de datos (DFD) a menudo son ideales para la búsqueda de amenazas.
- Los problemas tienden a seguir el flujo de datos, no el flujo de control.
- Utilizaremos estos diagramas para modelar los sistemas de red o la arquitectura de un software y luego buscar sus debilidades.
- Cuando se aplican en seguridad, a veces son llamados “Diagramas de modelo de amenazas”.

Modelado de amenazas: Análisis de reducción

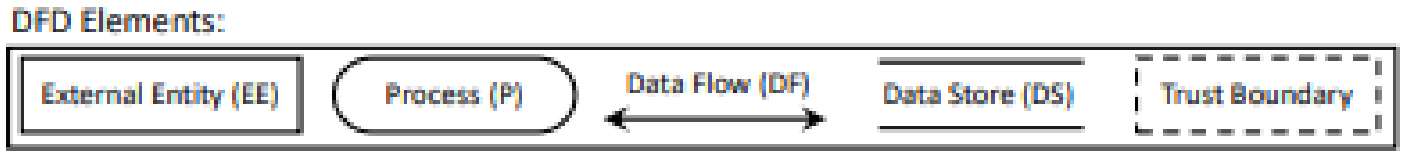
En el proceso de descomposición, se deben identificar cinco conceptos clave:

- **Límites de confianza:** Cualquier ubicación donde cambie el nivel de confianza o seguridad.
- **Rutas de flujo de datos:** El movimiento de datos entre ubicaciones.
- **Puntos de entrada:** Lugares donde se recibe entrada externa.
- **Operaciones privilegiadas:** Cualquier actividad que requiera mayores privilegios que la de una cuenta o proceso de usuario estándar, generalmente requerido para realizar cambios en el sistema o alterar la seguridad.
- **Detalles sobre la postura y el enfoque de seguridad:** La declaración de la política de seguridad, los fundamentos de seguridad y los supuestos de seguridad.

Desglosar un sistema en sus partes constituyentes hace que sea mucho más fácil identificar los componentes esenciales de cada elemento, así como tener en cuenta las vulnerabilidades y los puntos de ataque. Cuanto más entienda exactamente cómo funciona un programa, sistema o entorno, más fácil será identificar las amenazas.

Elementos de un DFD

Elemento	Apariencia	Significado	Ejemplos
Proceso	Rectángulo redondeado, círculo o círculos concéntricos	Cualquier código en ejecución	Código escrito en C, C#, Python, or PHP
Flujo de datos	Flecha	Comunicación entre procesos o entre procesos y almacén de datos	Conexiones de red, HTTP, RPC, LPC
Almacén de datos	Dos líneas paralelas con una etiqueta entre ellas	Cosas que almacenan datos	Archivos, Base de datos, el registro de Windows, segmentos de memoria compartida
Entidad externa	Rectángulo con esquinas afiladas	Persona, o código fuera de tu color	Tu cliente, una página web.



Ejemplo de un DFD

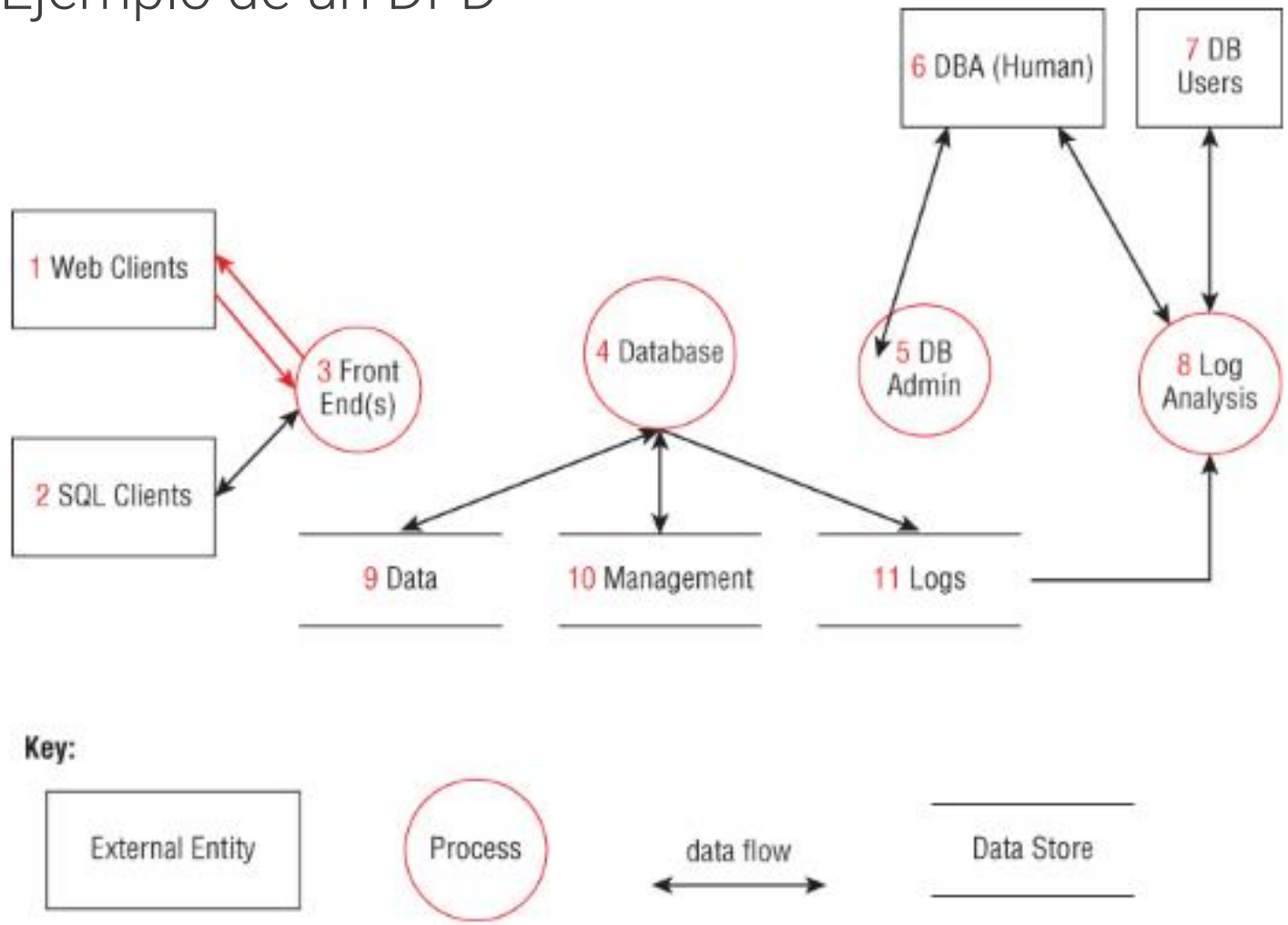
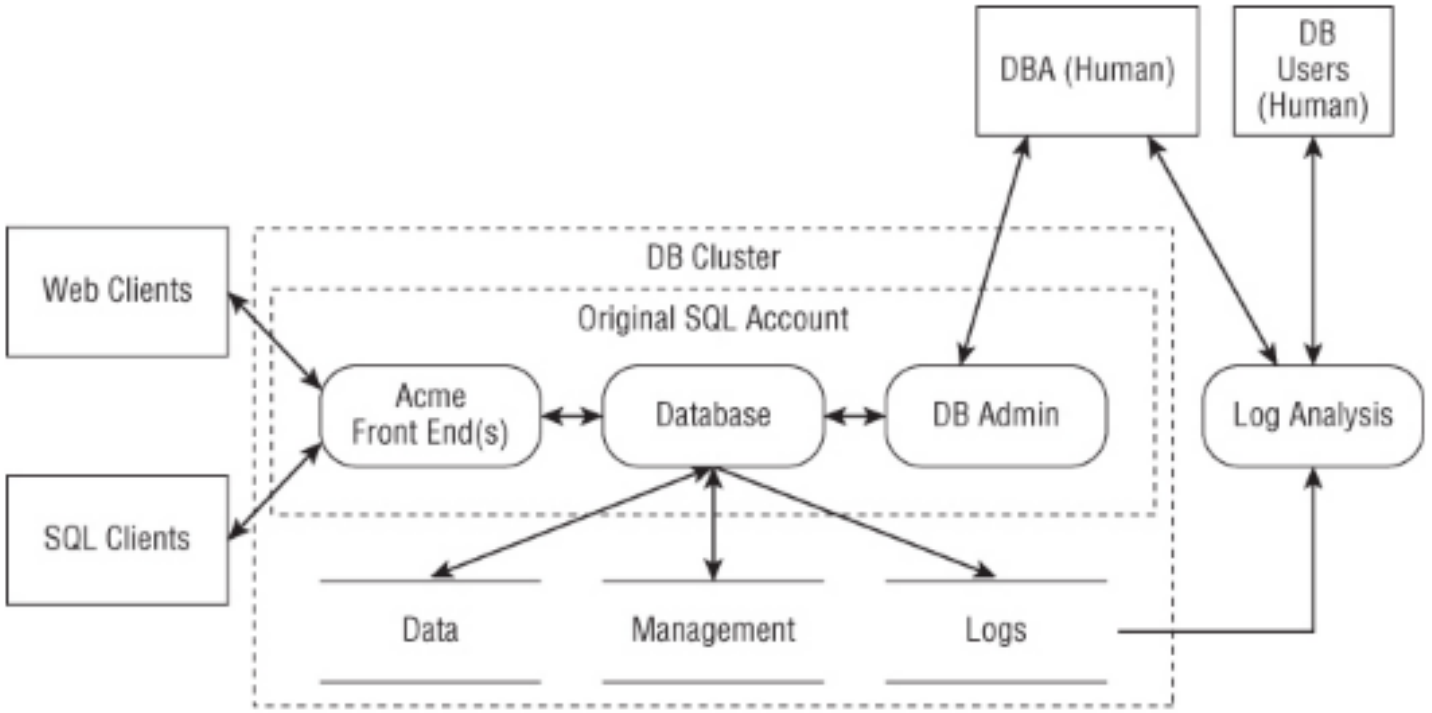


Figure 2.3 A classic DFD model



Key:

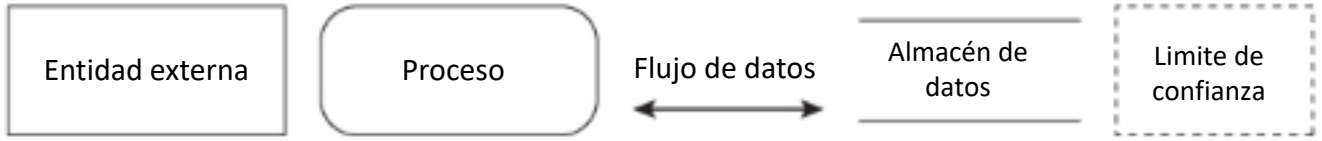


Figure 2.4 A modern DFD model (previously shown as Figure 2.1)

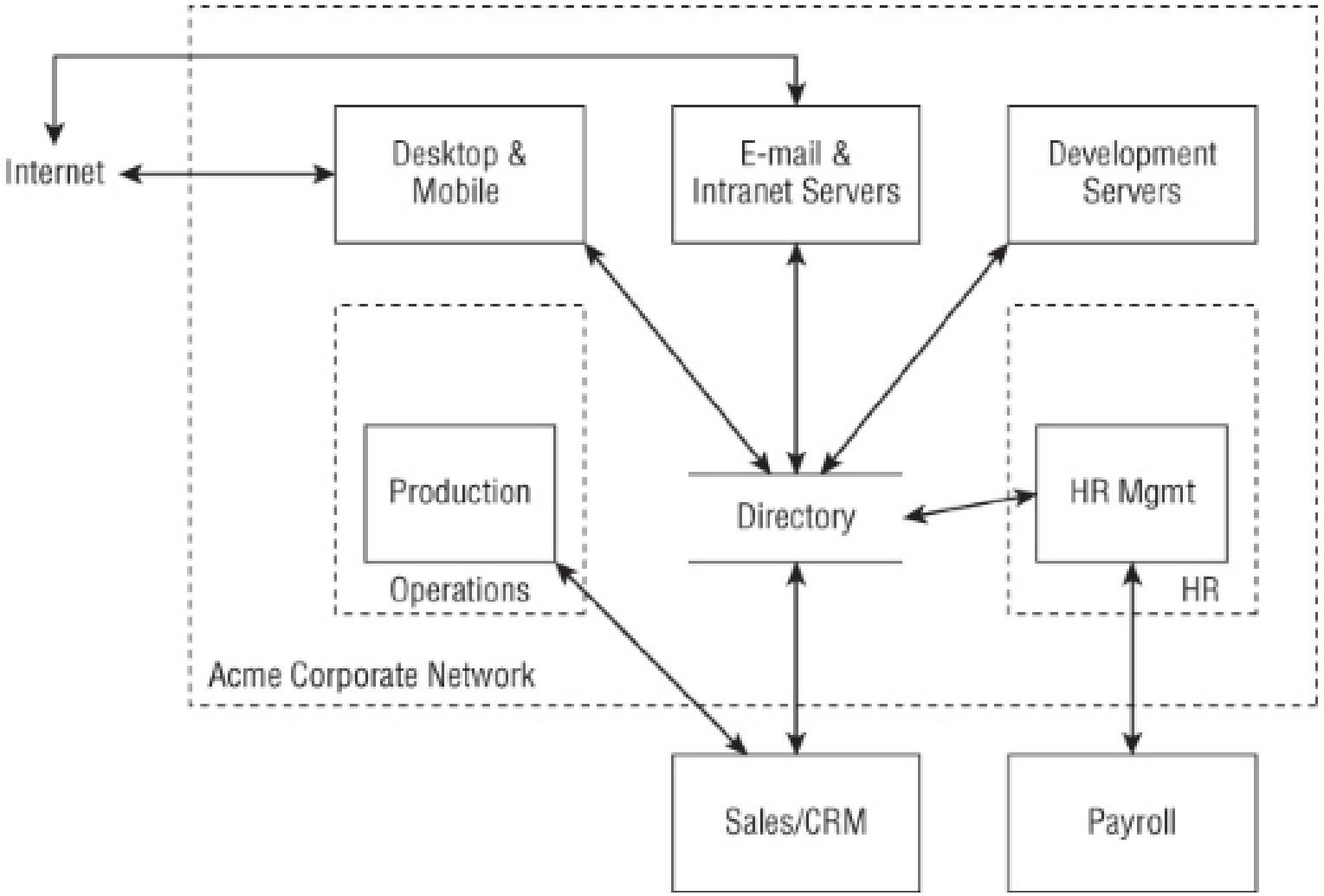


Figure 2.5 An operational network model

Priorización y respuesta

- Lo siguiente es documentar completamente las amenazas: definir los medios, el objetivo , consecuencias de una amenaza, técnicas necesarias para implementar una explotación, así como enumerar posibles contramedidas y controles.
- Clasifique o califique las amenazas: Existe una amplia gama de técnicas, como la clasificación de probabilidad × daño potencial, calificación alta / media / baja o el sistema DREAD.
  - La técnica de clasificación de probabilidad × potencial de daño produce un número de gravedad del riesgo en una escala de 1 a 100, con 100 el riesgo más grave posible.
  - El proceso de calificación alta / media / baja es aún más simple.

Priorización y respuesta

El sistema de calificación DREAD está diseñado para proporcionar una solución de calificación flexible que se basa en las respuestas a cinco preguntas principales sobre cada amenaza:

- *Damage potencial* (Potencial de daño): ¿qué tan grave es el daño si la amenaza se realiza?
- *Reproducibility* (Reproducibilidad): ¿qué tan complicado es para los atacantes reproducir el exploit?
- *Exploitability* (Explotabilidad): ¿qué tan difícil es realizar el ataque?
- *Affected users* (Usuarios afectados): ¿cuántos usuarios pueden verse afectados por el ataque (como porcentaje)?
- *Discoverability* (Descubrimiento): ¿Qué tan difícil es para un atacante descubrir la debilidad?

Al formular estas y otras preguntas personalizadas potencialmente adicionales, junto con la asignación de valores H / M / L (High / Medium / Low) o 3/2/1 a las respuestas, puede establecer una priorización detallada de amenazas.

Una vez que se establecen las prioridades de las amenazas, es necesario determinar las respuestas a esas amenazas. Las tecnologías y los procesos para remediar las amenazas se deben considerar y ponderar de acuerdo con su costo y efectividad. Las opciones de respuesta deben incluir hacer ajustes a la arquitectura del software, alterar las operaciones y los procesos, así como implementar componentes defensivos y detectivos.

Herramientas para el modelado de amenazas

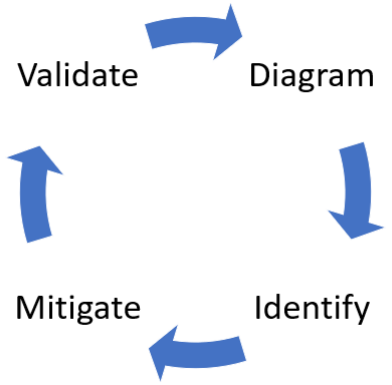
OWASP Threat Dragon

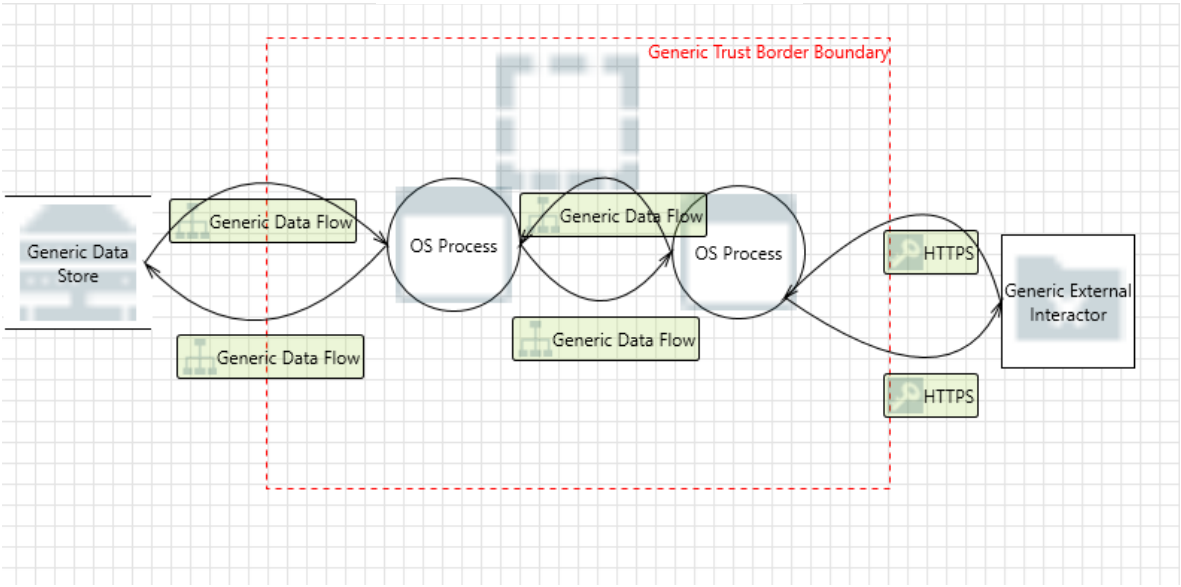
- Es una herramienta de modelado que se utiliza para crear diagramas de modelos de amenazas como parte de un ciclo de vida de desarrollo seguro.
- Sigue los valores y principios del manifiesto de modelado de amenazas (Ver apéndice).
- Se puede utilizar para:
  - Registrar posibles amenazas y decidir sobre sus mitigaciones
  - Dar una indicación visual de los componentes del modelo de amenazas y las superficies de las amenazas.
- Threat Dragon se ejecuta como una aplicación web o una aplicación de escritorio.

Herramientas para el modelado de amenazas

Microsoft Threat Modeling Tool

- La herramienta de modelado de amenazas es un elemento central del ciclo de vida de desarrollo de seguridad (SDL) de Microsoft.
- Permite que los arquitectos de software identifiquen y mitiguen posibles problemas de seguridad en forma temprana, cuando son relativamente fáciles y rentables de resolver.
- Como resultado, reduce en gran medida el costo total de desarrollo.





https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool

Actividad formativa 5: Modelado de amenazas

De algún sistema desarrollado o que conozca internamente en alguna asignatura o experiencia anterior, desarrolle el modelado de amenazas. Describa:

- El sistema y sus funcionalidades principales (3 líneas).
- Identifique activos de información mas valiosos (al menos 3).
- Identifique posible agentes de amenazas (al menos 1).
- Desarrolle el diagrama de amenazas con una de las herramientas anteriores, tomando en cuenta lo anterior.
- Priorice (de acuerdo a DREAD) las amenazas mas relevantes del sistema (de acuerdo a STRIDE) y fundamente por qué.

Escriba un post con lo anterior en el foro asociado y retroalimente al menos a un compañero

Bibliografía

1. Shostack, Adam. Threat Modeling. Wiley. Kindle Edition.
2. Threat Modeling Manifesto, https://www.threatmodelingmanifesto.org/
3. OWASP Threat Dragon, https://owasp.org/www-project-threat-dragon/

Manifiesto del modelado de amenaza

https://www.threatmodelingmanifesto.org/

Valores

- **Una cultura de búsqueda y resolución de problemas de diseño** por encima del cumplimiento de las casillas de verificación.
- **Personas y la colaboración** por encima de los procesos, metodologías y herramientas.
- **Un viaje de comprensión** en lugar de una instantánea de seguridad o privacidad.
- **Hacer un modelo de amenazas** en lugar de hablar de ello.
- **Perfeccionamiento continuo** en lugar de una sola entrega.

Principios

- El mejor uso del modelado de amenazas es mejorar la seguridad y la privacidad de un sistema mediante un análisis temprano y frecuente.
- El modelado de amenazas debe estar en consonancia con las prácticas de desarrollo de una organización y seguir los cambios de diseño en iteraciones que se limitan a partes manejables del sistema.
- Los resultados del modelado de amenazas son significativos cuando tienen valor para las partes interesadas.
- El diálogo es clave para establecer un entendimiento común que conduzca al valor, mientras que los documentos registran ese entendimiento y permiten la medición.

Manifiesto del modelado de amenaza

https://www.threatmodelingmanifesto.org/

Estos patrones son beneficiosos:

- Enfoque sistemático
- Creatividad informada
- Puntos de vista variados
- Conjunto de herramientas útiles
- De la teoría a la práctica

Estos NO:

- Héroe modelador de amenazas
- Admiración por el problema
- Tendencia a centrarse en exceso
- Representación perfecta

THREAT MODELING MANIFESTO

Lectura complementaria:
STRIDE-based Threat Modeling for Cyber-Physical Systems (2017)

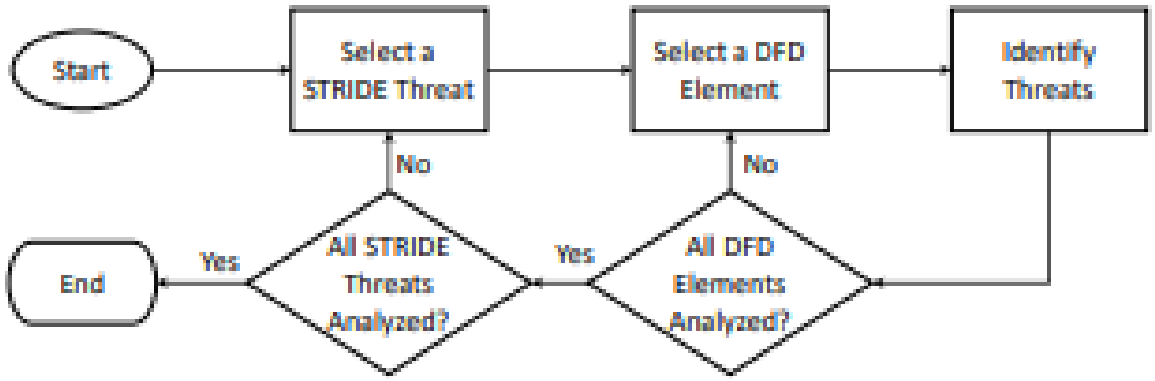


Figure 4. Threat analysis using STRIDE-per-element approach.

Table I
SUSCEPTIBILITY OF DFD ELEMENTS TO STRIDE THREATS.

DFD Element	S	T	R	I	D	E
Entity	✓		✓			
Data Flow		✓		✓	✓	
Data Store		✓	✓	✓	✓	
Process	✓	✓	✓	✓	✓	✓

(Khan et al, 2017)