DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

1.5. Introducción – Amenazas y su modelado

Fundamentos de ciberseguridad

Profesor

Juan Ignacio Iturbe A.

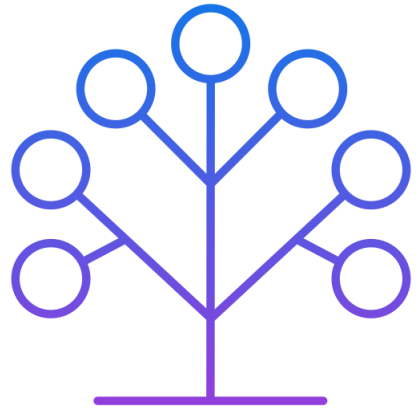
Tabla de contenidos

Resultado de aprendizaje

Evaluar los diferentes tipos de amenazas y vulnerabilidades en ciberseguridad, los ataques comunes y vectores de ataque, las tendencias emergentes en ciber amenazas y el impacto de la ingeniería social.

¿Qué es una Taxonomía?

- La palabra taxonomía deriva del griego taxis, que significa "ordenación o división", y nomos, que significa "ley".
- Por tanto, taxonomía significa "leyes de ordenación y división".
- En Internet se pueden encontrar muchas otras definiciones de la palabra, por ejemplo:
  - la ciencia de la clasificación según un sistema predeterminado (www.whatis.com)
  - la práctica y la ciencia de la clasificación (Wikipedia)
  - La ciencia de la categorización, o clasificación, de las cosas basada en un sistema predeterminado (www.webopedia.com)



What is taxonomy? – An overview with myriapodological examples, 2009

Conceptos: Amenaza vs Ataque

Categoría	Amenaza (Threat)	Ataque (Attack)
Definición	Potencial causa de un incidente no deseado que puede resultar en daño a un sistema o una organización.	Intento de destruir, exponer, alterar, inhabilitar, robar u obtener un acceso no autorizado para usar un activo de manera no autorizada.
Naturaleza	Potencial o latente.	Activa y manifestada.
Ejemplo	Filtración de datos	Un ataque de phishing donde un actor malicioso envía un correo electrónico falso.
Causa/Origen	Pueden ser humanos (hackers, empleados descontentos), naturales (terremotos, inundaciones) o técnicos (errores en el software).	Normalmente surge de una amenaza cuando se lleva a cabo la acción maliciosa.
Relación con vulnerabilidades	Se relaciona con vulnerabilidades en el sentido de que una vulnerabilidad puede ser explotada por una amenaza.	Es el resultado directo de aprovechar una vulnerabilidad.
Prevención/ Mitigación	Estrategias proactivas para identificar y evaluar potenciales amenazas, como análisis de riesgo y formación de empleados.	Estrategias reactivas para responder y remediar el daño causado.

Repasemos conceptos claves con un ejemplo

Escenario:

Pedro trabaja en el departamento de Recursos Humanos de una empresa mediana. Una mañana, mientras revisa su bandeja de entrada, encuentra un correo electrónico con el asunto "Verificación de Seguridad del Banco Nacional". El correo parece provenir del banco donde la empresa tiene sus cuentas corporativas.

El mensaje indica que, debido a intentos recientes de acceso no autorizado, es esencial que todos los titulares de cuentas verifiquen su identidad haciendo clic en un enlace proporcionado. El diseño del correo es idéntico al del "Banco Nacional" con logos, colores y fuentes que parecen auténticos. Sin embargo, al pasar el cursor sobre el enlace, Pedro nota que la URL no corresponde al dominio oficial del banco, sino a una dirección web sospechosa.

Intrigado, Pedro decide informar a su equipo de TI sobre el correo recibido.

Identifique:

- Amenaza
- Ataque
- Vector de ataque
- Agente de amenaza

¿Cómo prevenir este tipo de ataques en tu organización?

Taxonomías de amenazas y ataques

Algunas taxonomías de amenazas y ataques son:

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

Profundicemos en algunas de estas…

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

Dominio de ataque (3000)

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

¿Es posible protegerse sobre el panorama completo de amenazas?

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

Ejemplo: CAPEC
(https://capec.mitre.org/)

Dominio de ataque

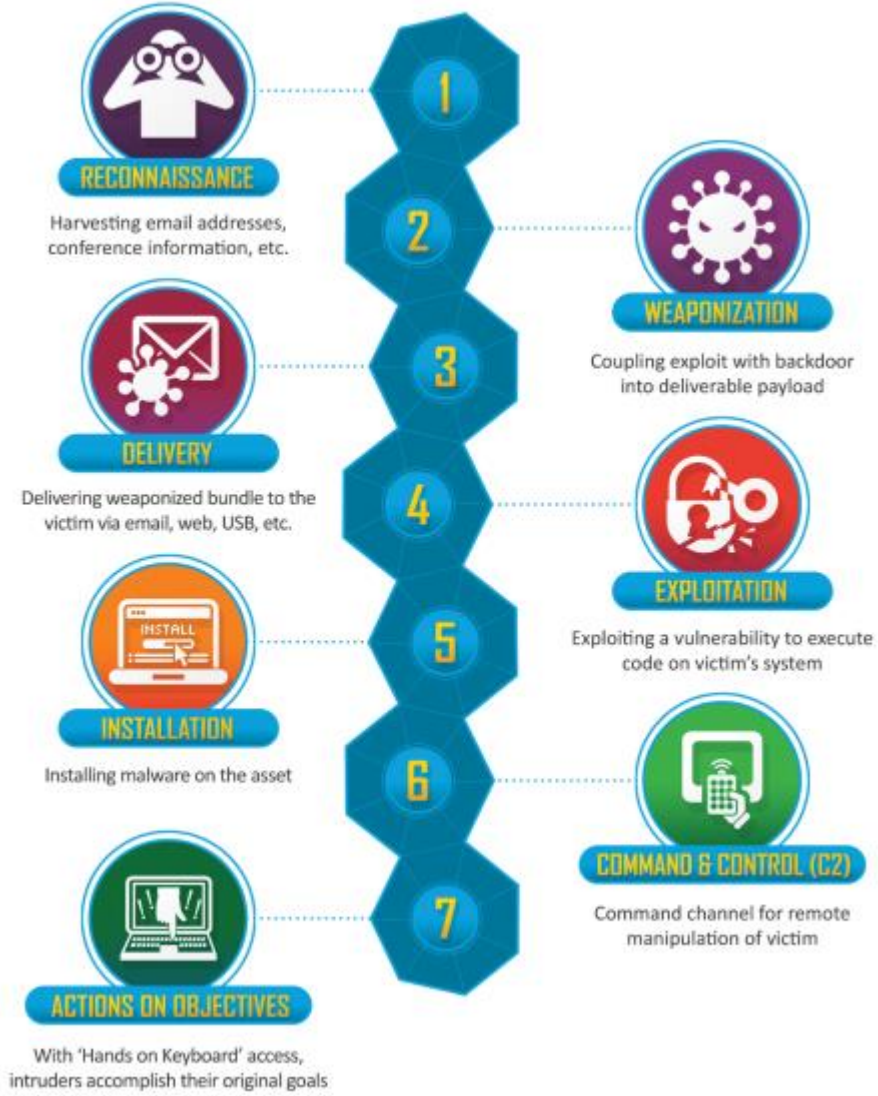
- Ingeniería social (403)
  - Inyección de Parámetros - (137)
  - Suplantación de Identidad - (151)
  - Suplantación de Ubicación de Recursos - (154)
  - Suplantación de Acción - (173)
  - Ataque a la integridad del software - (184)
  - Elicitación de Información - (410)
  - **Manipular el Comportamiento Humano - (416)**
  - Obstrucción - (607)
  - Suplantación de Metadatos - (690)

- Manipular el Comportamiento Humano - (416)
  - Pretexto
  - Influencia Percepción
  - Influencia en el Objetivo a través del Enmarcamiento
  - Influencia a través de Principios Psicológicos
  - Influencia mediante incentivos
    - **Probabilidad de ataque:** Baja
    - **Severidad típica:** Baja
    - **Prerrequisitos:**
      - El adversario debe tener los medios y el conocimiento de cómo comunicarse con el objetivo de alguna manera.
      - El adversario debe tener conocimiento de los incentivos que influirían en las acciones del objetivo específico.
    - **Habilidad requerida**: Baja
      - El adversario requiere grandes dotes interpersonales y de comunicación.
    - **Consecuencias:** Confidencialidad, Disponibilidad, Integridad
    - **Mitigaciones:**
      - Una organización debe proporcionar a sus empleados una formación regular y sólida en ciberseguridad para prevenir los ataques de ingeniería social.

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

¿Cómo utilizarías el conocimiento de este modelo para prevenir ataques en tu organización?



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®

Ejemplo: uso del MITRE ATT&CK Framework

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) ha identificado una nueva campaña de malware. En ella, el atacante busca persuadir a las personas de descargar un archivo adjunto y ejecutarlo en su equipo, donde gatillará una infección con malware. Para lograr persuadir a su víctima, el mensaje del correo indica falsamente que se envió un nuevo pedido, el que se adjunta, siendo dicho archivo realmente un programa malicioso.

Familia de malware: FormBook (MSExcel/CVE_2017_11882)

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto.

IoC Correo Electrónico

- Datos del encabezado del correo
- Correo electrónico: office@altaskalp.com

Servidor de correo

- mail0.altaskalp.com [147.182.182.229]

Asunto

- NUEVA ORDEN DE COMPRA

IoC Archivo

- Archivos que se encuentran en la amenaza
- Nombre: NUEVA ORDEN DE COMPRA.xlsx
- SHA256: aefbd29fa01b6796341be145648ff5d0c776752cdf526865a88e70e20ae32bc2

IoC Red

- www.yukotopia[.]com/dy26

MITRE ATT&CK

T1106: Native API
T1129: Shared Modules
T1203: Exploitation for Client Execution (link)
T1055: Process Injection
T1014: Rootkit
T1036: Masquerading
T1497: Virtualization/Sandbox Evasion
T1140: Deobfuscate/Decode Files or Information
T1027: Obfuscated Files or Information
T1027.002: Software Packing
T1057: Process Discovery
T1018: Remote System Discovery
T1083: File and Directory Discovery
T1082: System Information Discovery
T1056.004: Credential API Hooking
T1560: Archive Collected Data
T1115: Clipboard Data
T1573: Encrypted Channel
T1105: Ingress Tool Transfer
T1095: Non-Application Layer Protocol
T1071: Application Layer Protocol
T1529: System Shutdown/Reboot

Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los antispam y sandboxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

¿Se consideran estas precauciones en tu organización?

https://www.csirt.gob.cl/alertas/2cmv21-00254-01/

Cyber Kill Chain vs. MITRE ATT&CK

Característica	Cyber Kill Chain	MITRE ATT&CK
Objetivo principal	Describir las etapas de un ataque desde inicio hasta ejecución.	Enumerar y explicar tácticas y técnicas usadas por adversarios.
Enfoque	Lineal, representa las etapas consecutivas de un ataque.	Matriz, aborda tácticas y técnicas en diferentes escenarios de ataque.
Detallado	Más general, centrado en fases.	Más detallado, con información específica sobre tácticas y técnicas.
Aplicabilidad	Mejor para entender la progresión del ataque.	Mejor para defensa activa y simulación de adversarios (red teaming).
Adaptabilidad	Menos adaptable a nuevos tipos de ataques.	Muy adaptable y en constante actualización con nuevas técnicas.
Actualizaciones	No es comúnmente actualizado con nuevas fases.	Regularmente actualizado con nuevos hallazgos e investigaciones.
Integración con herramientas	Menos integrado con soluciones modernas de ciberseguridad.	Muchas soluciones modernas se integran o usan ATT&CK para describir amenazas.

STRIDE

- STRIDE es un modelo de amenazas desarrollado por Microsoft para ayudar a identificar posibles amenazas a la seguridad en el diseño de un sistema o aplicación.
- Este modelo ayuda a los ingenieros y diseñadores de software a pensar en la seguridad desde el principio y durante todo el ciclo de vida del desarrollo del software.
- Aunque STRIDE generalmente se usa para enfocarse en las amenazas de la aplicación, es aplicable a otras situaciones, como las amenazas de red y las amenazas de host.
- En general, el propósito de STRIDE y otras herramientas en el modelado de amenazas es considerar la mayoría de las preocupaciones y enfocarse en el objetivo o los resultados finales de un ataque.
- Intentar identificar todos y cada uno de los métodos y técnicas de ataque específicos es una tarea imposible: constantemente se desarrollan nuevos ataques.
- Aunque los objetivos o propósitos de los ataques se pueden clasificar y agrupar libremente, permanecen relativamente constantes con el tiempo.

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.
Tampering (Manipulación)	Integridad	Cualquier acción que resulte en cambios no autorizados o manipulación de datos, ya sea en tránsito o en almacenamiento.
Repudiation (Repudio)	No repudiación	La capacidad de un usuario o atacante de negar haber realizado una acción o actividad
Information disclosure (Divulgación de información)	Confidencialidad	La revelación o distribución de información privada, confidencial o controlada a entidades externas o no autorizadas.
Deny of Service, DoS (Denegación de servicio)	Disponibilidad	Un ataque que intenta evitar el uso autorizado de un recurso.
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.

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

Resumen

Característica / Marco	MITRE ATT&CK	CAPEC	Cyber Kill Chain	STRIDE
Enfoque principal	Tácticas, técnicas y procedimientos de adversarios.	Patrones comunes de ataques.	Fases de un ataque cibernético.	Amenazas a la seguridad en diseño y arquitectura.
Uso principal	Detección y respuesta a incidentes, simulación de adversarios.	Diseño y prueba de software seguro.	Inteligencia de amenazas, detección de intrusos.	Diseño de software y sistemas seguros.
Granularidad	Detallado con técnicas específicas y ejemplos.	Detallado con patrones y técnicas.	General, centrado en fases.	General, categorizado por tipo de amenaza.
Actualizaciones	Regularmente con nuevos hallazgos.	Regularmente.	No es comúnmente actualizado.	No es comúnmente actualizado.
Aplicación	Defensa activa, red teaming.	Desarrollo seguro, pentesting.	Inteligencia de amenazas, defensa.	Desarrollo y diseño seguro.
Componentes	Matriz de tácticas y técnicas.	Lista de patrones de ataques.	7 fases de ataques.	Tipos de amenazas (Spoofing, Tampering, etc.).

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. ¿Cuándo y donde podrían ellos atacarnos?

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

Características del 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

Pasos comunes de las metodologías de modelado de amenaza

1. Identificar los objetos en el sistema bajo consideración
2. Identificar los flujos entre estos objetos
3. Identificar los activos de interés
4. Identificar las debilidades y vulnerabilidades del sistema
5. Identificar amenazas
6. Determinar explotabilidad

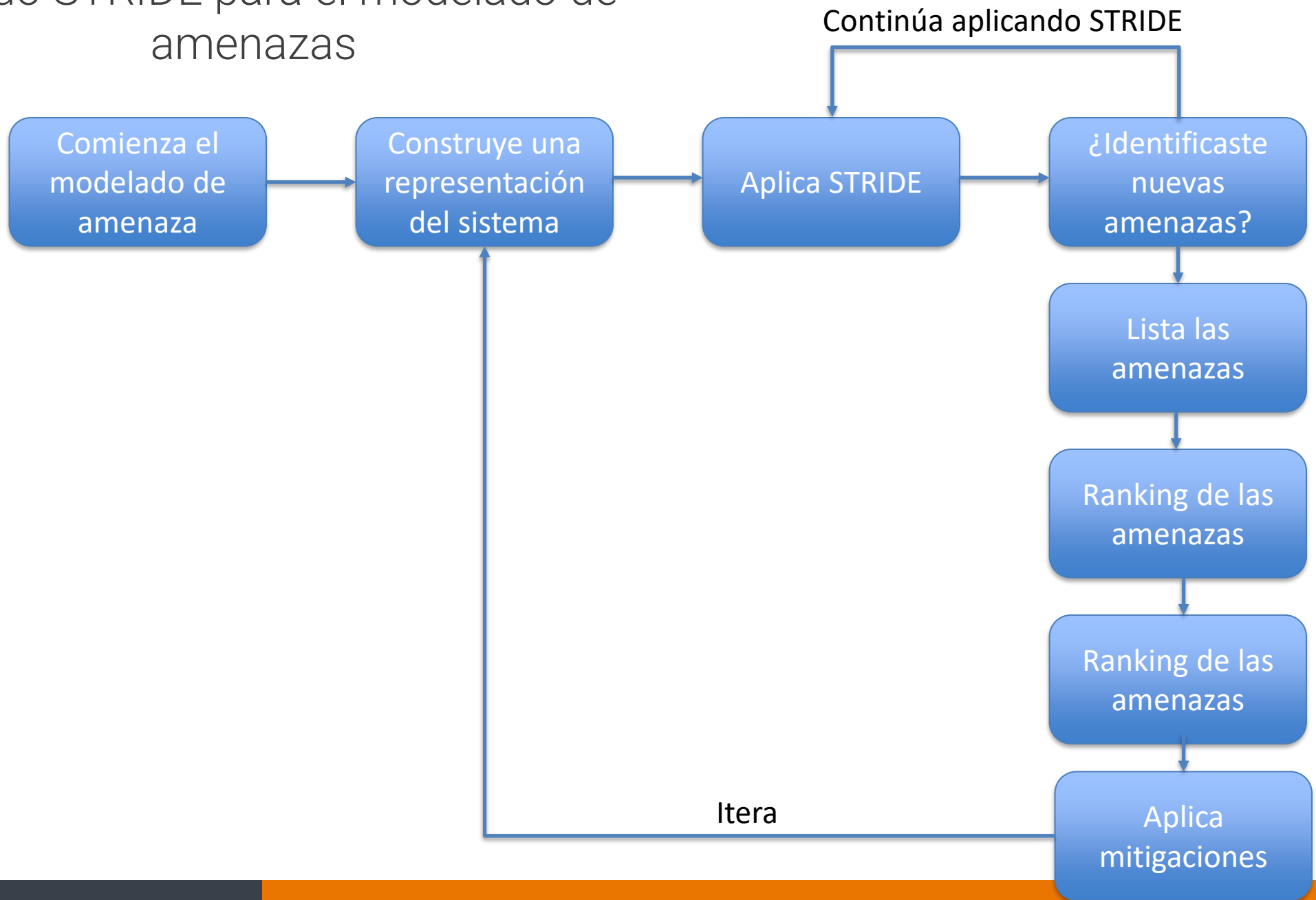
Threat Modeling – A practical Guide for Development Teams, 2020

Existen varias metodologías o marcos de trabajo para modelar amenazas

- STRIDE
- STRIDE por elemento
- STRIDE por interacciones
- Process for Attack Simulation and Threat Analysis (PASTA)
- Threat Assessment and Remediation Analysis (TARA)
- Trike
- LINDUNN (Amenazas a la privacidad)
- Security and Privacy Architecture Through Risk-Driven Threat Assessment (SPARTA)
- Incluso hay juegos (Elevation of privilege, OWASP Cornucopia, etc)

Threat Modeling – A practical Guide for Development Teams, 2020

Usando STRIDE para el modelado de amenazas

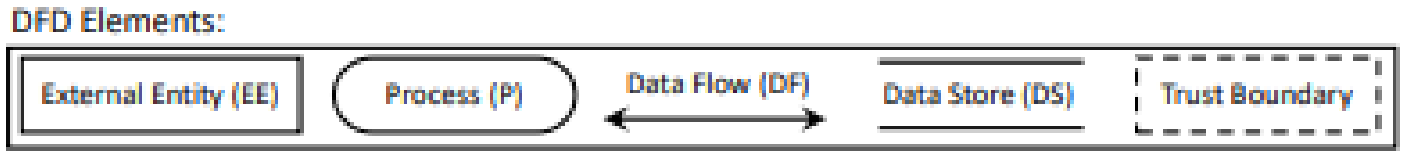


Uso de DFD en el modelado de amenazas

- 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”.

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.



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.

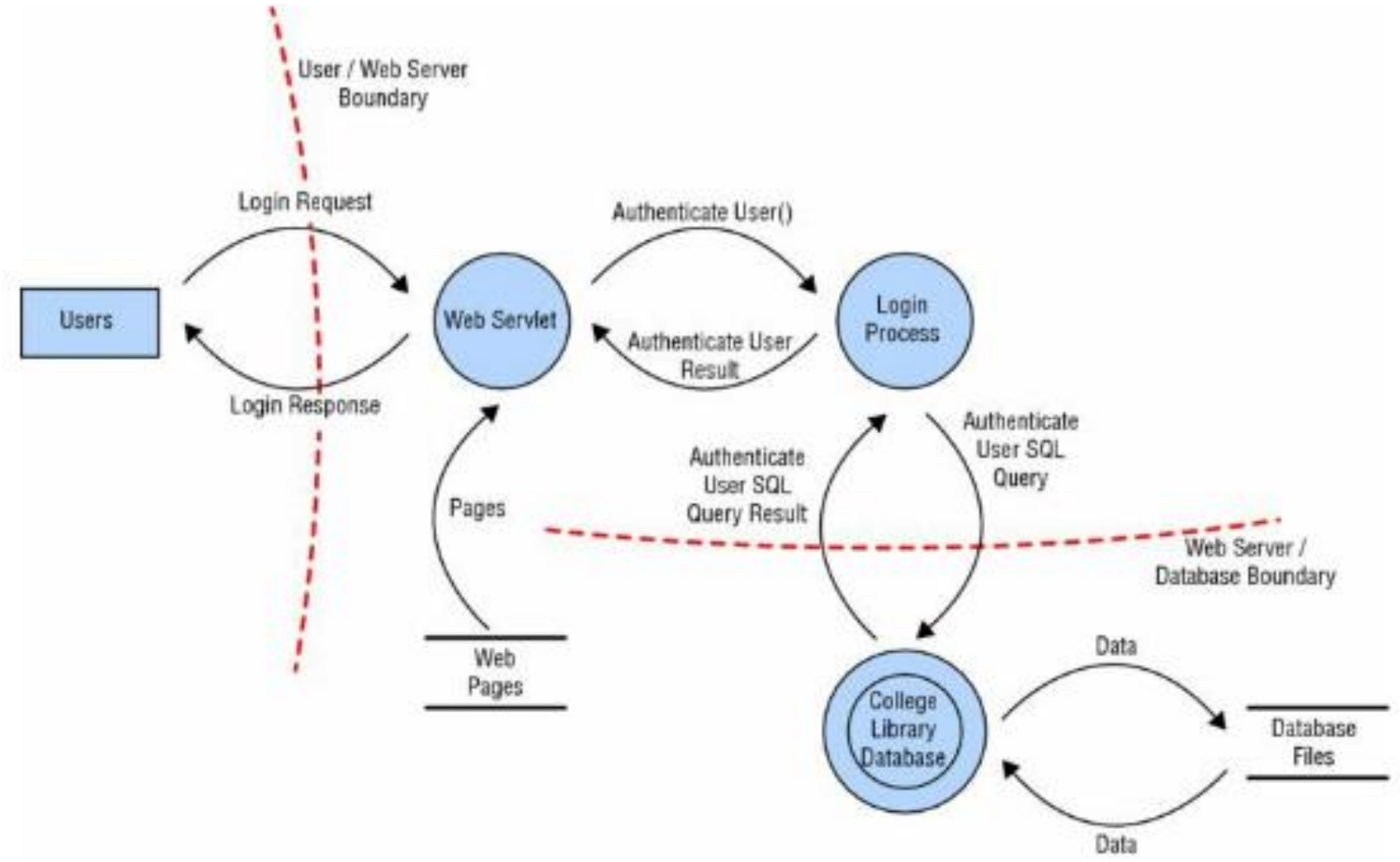
Desglosar un sistema en sus partes constituyentes hace que sea mucho más fácil identificar los componentes esenciales de cada elemento, así como tener en cuenta las vulnerabilidades y los puntos de ataque. Cuanto más entienda exactamente cómo funciona un programa, sistema o entorno, más fácil será identificar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

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 más 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



Ejemplo de un DFD

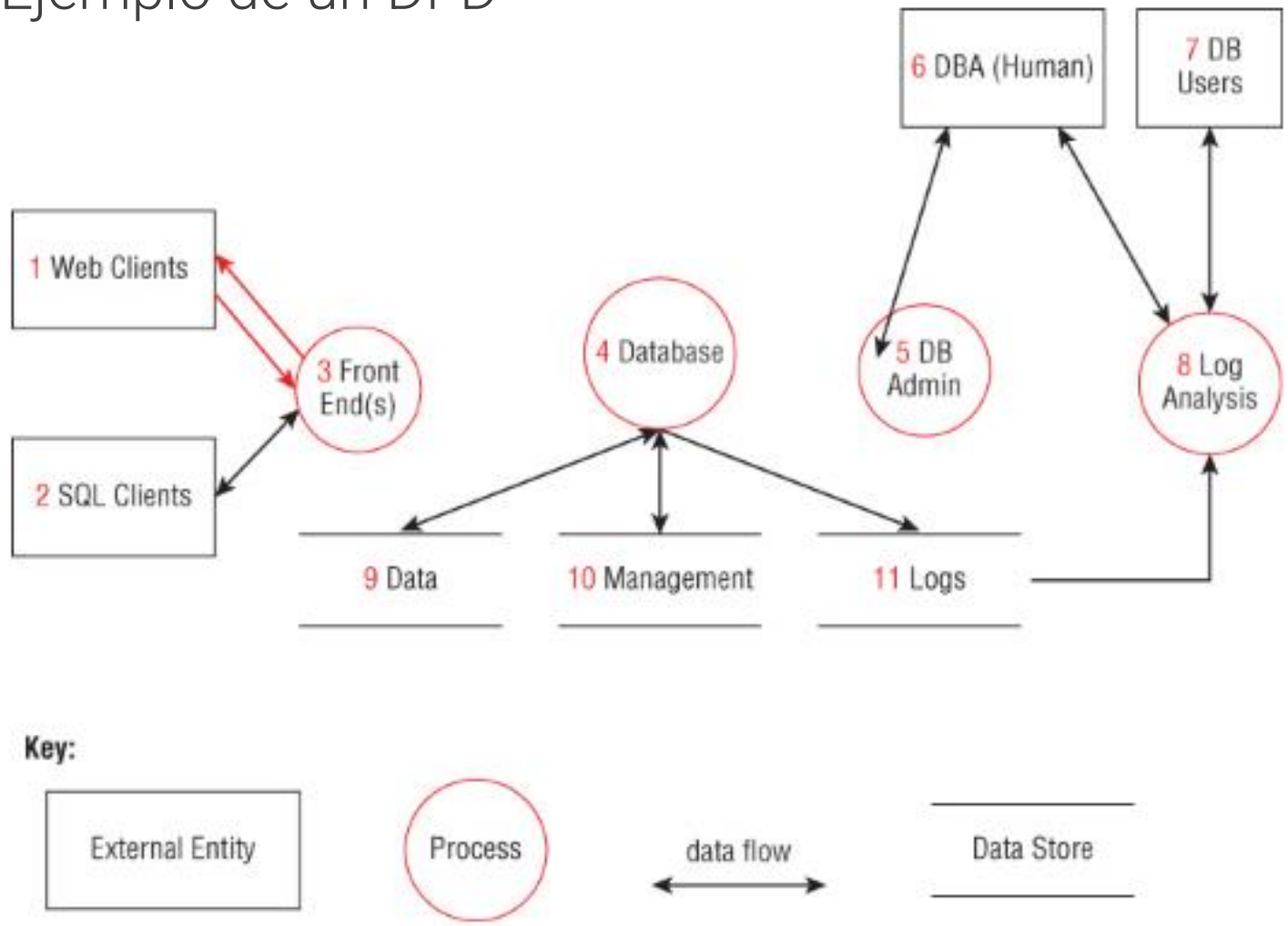
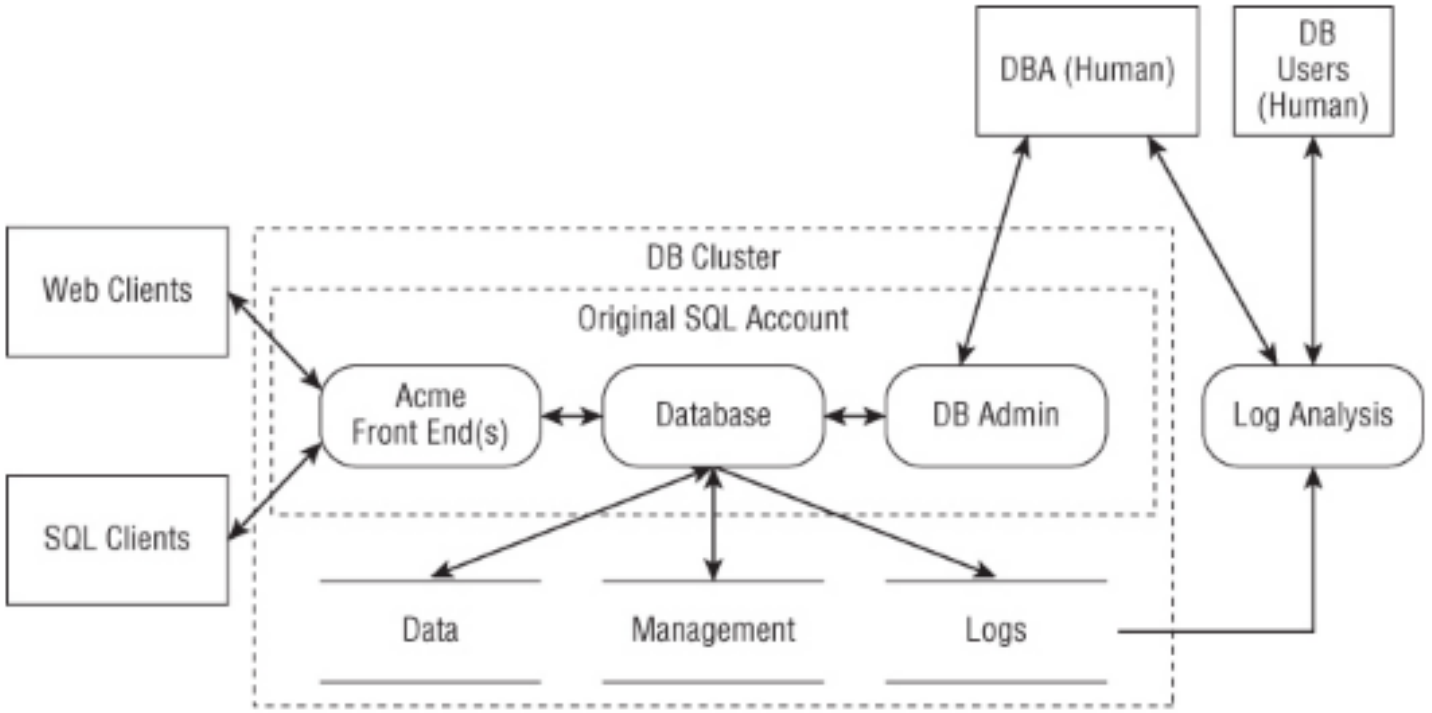


Figure 2.3 A classic DFD model



Key:

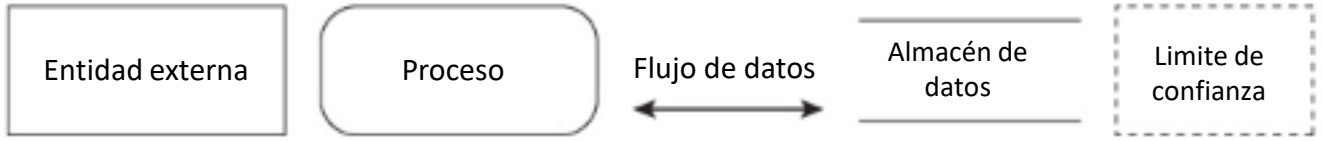


Figure 2.4 A modern DFD model (previously shown as Figure 2.1)

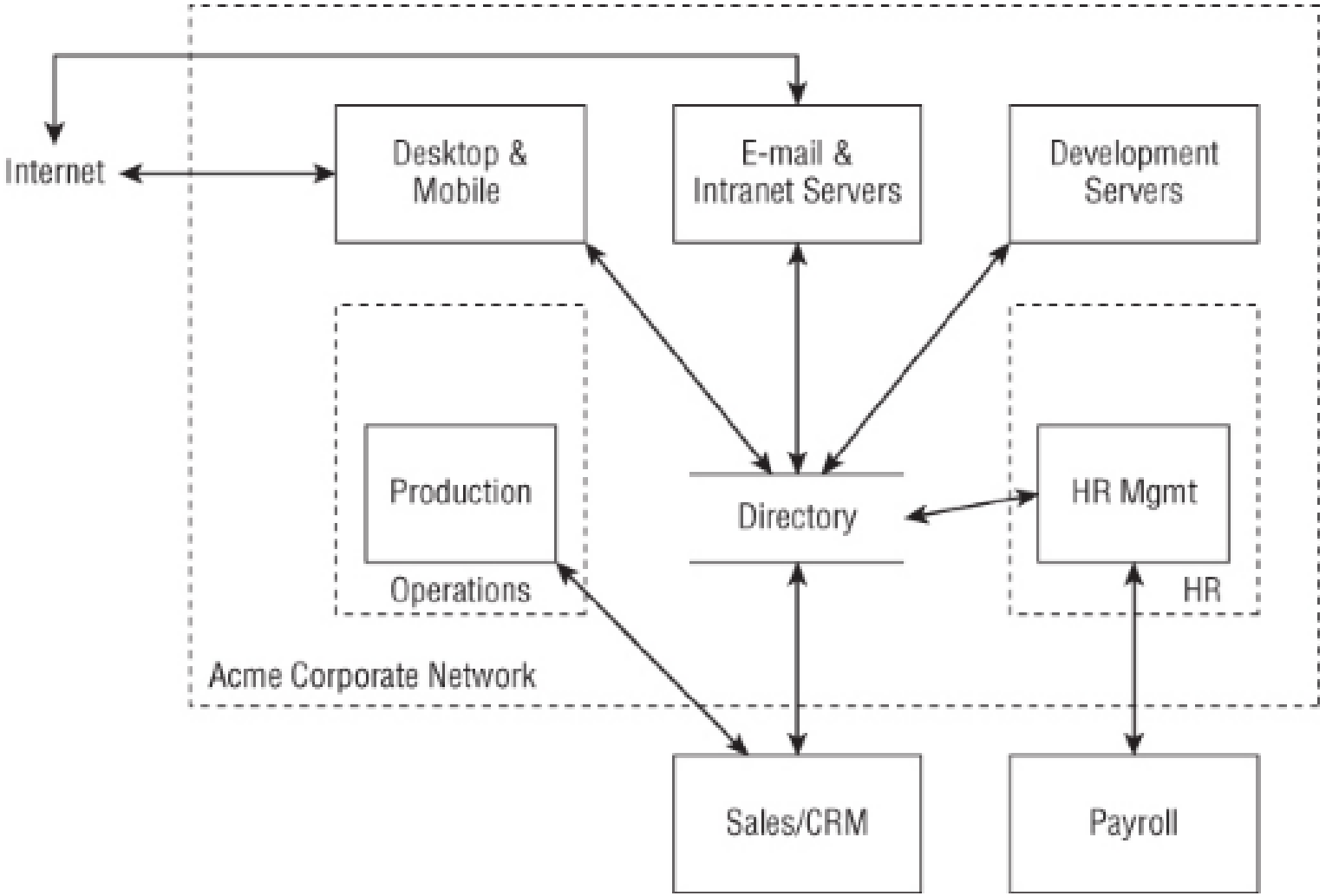
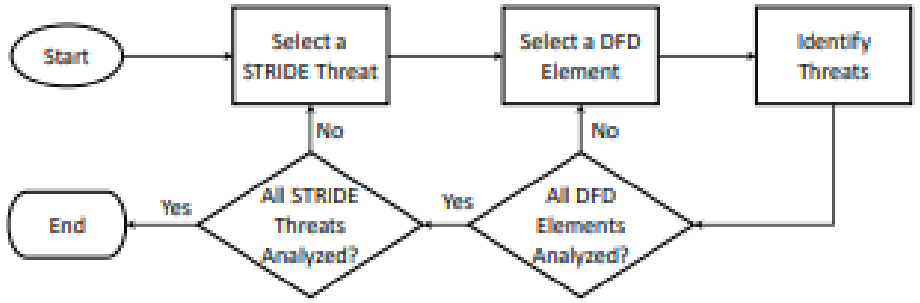


Figure 2.5 An operational network model

Usando STRIDE por cada elemento

- Variación de STRIDE desarrollada por Michael Howard and Shawn Hernan.
- Agrega estructura para manejar la falta de límites de STRIDE (por la observación de ciertos elementos que son más susceptibles a amenazas específicas que otros).



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

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

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): ¿Es el ataque potencial fácilmente reproducible?
- *Exploitability* (Explotabilidad): ¿Cuan fácil es ejecutar este ataque de forma exitosa?
- *Affected users* (Usuarios afectados): ¿Qué porcentaje de la población de usuarios se verían impactados?
- *Discoverability* (Descubrimiento): ¿Si el adversario actualmente no conoce el ataque potencial, cual es la probabilidad que ellos lo descubran?

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

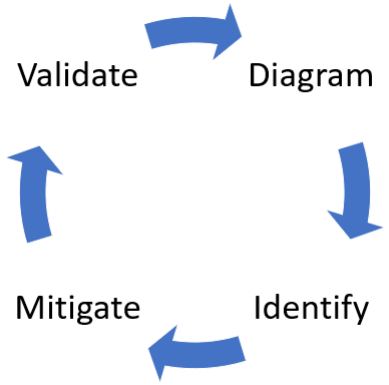
OWASP Threat Dragon

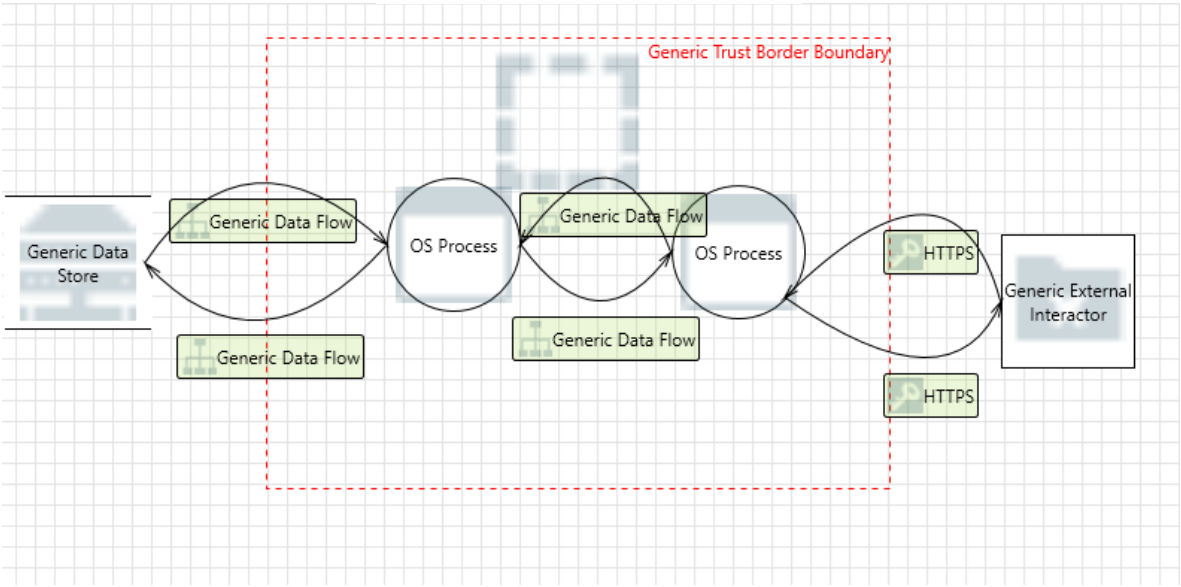
- Es una herramienta de modelado que se utiliza para crear diagramas de modelos de amenazas como parte de un ciclo de vida de desarrollo seguro.
- Sigue los valores y principios del manifiesto de modelado de amenazas (Ver apéndice).
- Se puede utilizar para:
  - Registrar posibles amenazas y decidir 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: Modelado de amenazas

Del caso de estudio “BankSecure”, desarrolle el modelado de amenazas. Describa:

- Identifique activos de información más valiosos.
- Identifique posibles agentes de amenazas.
- Desarrolle el diagrama de amenazas con una de las herramientas anteriores, tomando en cuenta lo anterior.
- Priorice (de acuerdo a DREAD) las amenazas más relevantes del sistema (de acuerdo a STRIDE) y fundamente por qué.

- Suba lo desarrollado al curso en usachvirtual individualmente.

Bibliografía

1. Shostack, Adam. Threat Modeling. Wiley. Kindle Edition.
2. Tarandach et al. Threat Modeling: A Practical Guide for Development Teams. O'Reilly.
3. Threat Modeling Manifesto, https://www.threatmodelingmanifesto.org/
4. OWASP Threat Dragon, https://owasp.org/www-project-threat-dragon/

Próxima sesión…

- Gestión del riesgo cómo un elemento clave en la evaluación y planeación de la ciberseguridad.
- Requisitos que debe tener una gestión del riesgo efectiva.
- Características de la gestión del riesgo.
- Metodologías de gestión de riesgos.
- Análisis de riesgos cualitativo y cuantitativo.

ANEXOS

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

STRIDE en detalle

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.

MITRE CVE

https://cve.mitre.org/

- La misión del programa CVE es identificar, definir y catalogar las vulnerabilidades de ciberseguridad de dominio público.
- Existe un registro CVE para cada vulnerabilidad del catálogo.
- Las vulnerabilidades son descubiertas, asignadas y publicadas por organizaciones de todo el mundo que se han asociado al programa CVE.
- Los socios publican registros CVE para comunicar descripciones coherentes de vulnerabilidades.
- Los profesionales de las tecnologías de la información y de la ciberseguridad utilizan los registros CVE para coordinar sus esfuerzos para priorizar y abordar las vulnerabilidades.

Inteligencia de amenazas
UNE-EN ISO/IEC 27002

- **Control:** La información relativa a las amenazas a la seguridad de la información debería recopilarse y analizarse para producir información sobre amenazas.
- **Propósito:** Proporcionar conocimiento del entorno de amenazas de la organización para que puedan ser adoptadas las acciones de mitigación apropiadas.
- **Orientación:**
  - La información sobre amenazas existentes o emergentes se recoge y analiza para:
    - a) facilitar acciones fundamentadas para evitar que las amenazas causen daños a la organización;
    - b) reducir el impacto de dichas amenazas