Desarrollo Seguro de Software

Diseño Seguro de Software

Unidad temática Nro. 400

Docentes:

- Alonzo, Maximiliano (maximiliano.alonzo@ucu.edu.uy)
- Canedo, Gerardo (gerardo.canedo@ucu.edu.uy)

Introducción a diseño seguro de software

Modelado de Amenazas

Unidad temática Nro. 4.1

Diseño ad-hoc y la seguridad

- Con frecuencia, los sistemas se diseñan de forma *ad-hoc*, sin una planificación estructurada.
- En este escenario, la seguridad del sistema se convierte en una víctima del caos y la falta de consideración adecuada.

Importancia del Modelado de Amenazas

- El Modelado de Amenazas proporciona una metodología efectiva para estructurar el diseño de sistemas desde una perspectiva de seguridad específica.
- Su objetivo principal es reducir el caos y mejorar la seguridad al identificar y abordar de manera sistemática las posibles amenazas y riesgos.

Introducción a diseño seguro de software

El Modelado de Amenazas es un proceso continuo de análisis y evaluación de riesgos de seguridad que resulta fundamental para:

- Identificar los riesgos de seguridad asociados al software de manera integral y en un nivel alto.
- Comprender cómo podrían materializarse los posibles ataques.
- Proporcionar un enfoque estructurado y formal para abordar la seguridad del software.
- Facilitar un ejercicio de pensamiento y análisis con el objetivo de descubrir vulnerabilidades y riesgos potenciales.
- Tomar decisiones informadas para fortalecer la seguridad del software.

Modelado de Amenazas (alto nivel)

- Las fallas de diseño generan el 50% de las vulnerabilidades. Estas fallas no pueden ser detectadas a partir del código fuente.
- El modelado de amenazas consiste en identificar riesgos técnicos, evaluarlos y determinar la forma de tratarlos.
- En necesario priorizar los riesgos identificados ya que no todos tienen la misma criticidad para el negocio.
- Esta actividad se realizar de forma periódica y se gestionan métricas comparables.

Nota importante de Nomenclatura

Modelado de Amenazas = Análisis de Riesgos

Distintos autores denominan la misma actividad de distintas formas:

Modelado de Amenazas → Microsoft
Análisis de Riego → Gary McGraw

Tratarlos como sinónimos.

Características del Modelado de Amenazas

Modelado de Amenazas

Unidad temática Nro. 4.1.1

UCU

Características del Modelado de Amenazas

Mejora la estructura del diseño

- El Modelado de Amenazas es el método principal para identificar y prevenir defectos de diseño en el software.
- Aporta una estructura y organización sólida al proceso de diseño del sistema, lo que ayuda a minimizar la posibilidad de fallas y vulnerabilidades.
- Permite analizar minuciosamente la arquitectura y los componentes del sistema, asegurando la detección y mitigación de posibles vulnerabilidades.

Características del Modelado de Amenazas

Mejora la comprensión de la aplicación

- Al representar las estructuras, interacciones, flujos de datos y controles relevantes, se realiza un ejercicio que fomenta una comprensión más profunda de los componentes, protocolos y tecnologías involucradas.

Características del Modelado de Amenazas

Posibilita la identificación temprana de riesgos

- El Modelado de Amenazas es un enfoque efectivo para identificar y detectar fallas en el diseño del software.
- Al adoptar una postura crítica, se pueden descubrir potenciales riesgos de seguridad en etapas tempranas del desarrollo, lo que permite abordarlos de manera proactiva, permitiendo su mitigación o prevención efectiva.

Características del Modelado de Amenazas

Facilita la comunicación entre diseñadores y desarrolladores

- Proporciona un lenguaje común y una representación visual clara de los posibles riesgos y vulnerabilidades, lo que ayuda a alinear los esfuerzos de seguridad.
- Fomenta una comunicación clara, efectiva y colaborativa entre los diseñadores y los desarrolladores de software sobre los aspectos de seguridad del sistema, lo que ayuda a alinear los esfuerzos de seguridad.

Características del Modelado de Amenazas

Apoyo al Testing de Seguridad

- Es una valiosa herramienta para el Testing de Seguridad.
- Proporciona una base sólida para identificar los escenarios de prueba más relevantes y diseñar pruebas efectivas que evalúen la resistencia del software ante posibles ataques.

Características del Modelado de Amenazas

Requiere tiempo y dedicación

- Así como el diseño o el modelado UML, el Modelado de Amenazas también puede ser una actividad enriquecedora y, aunque pueda resultar divertida, requiere tiempo y dedicación para llevarla a cabo correctamente.

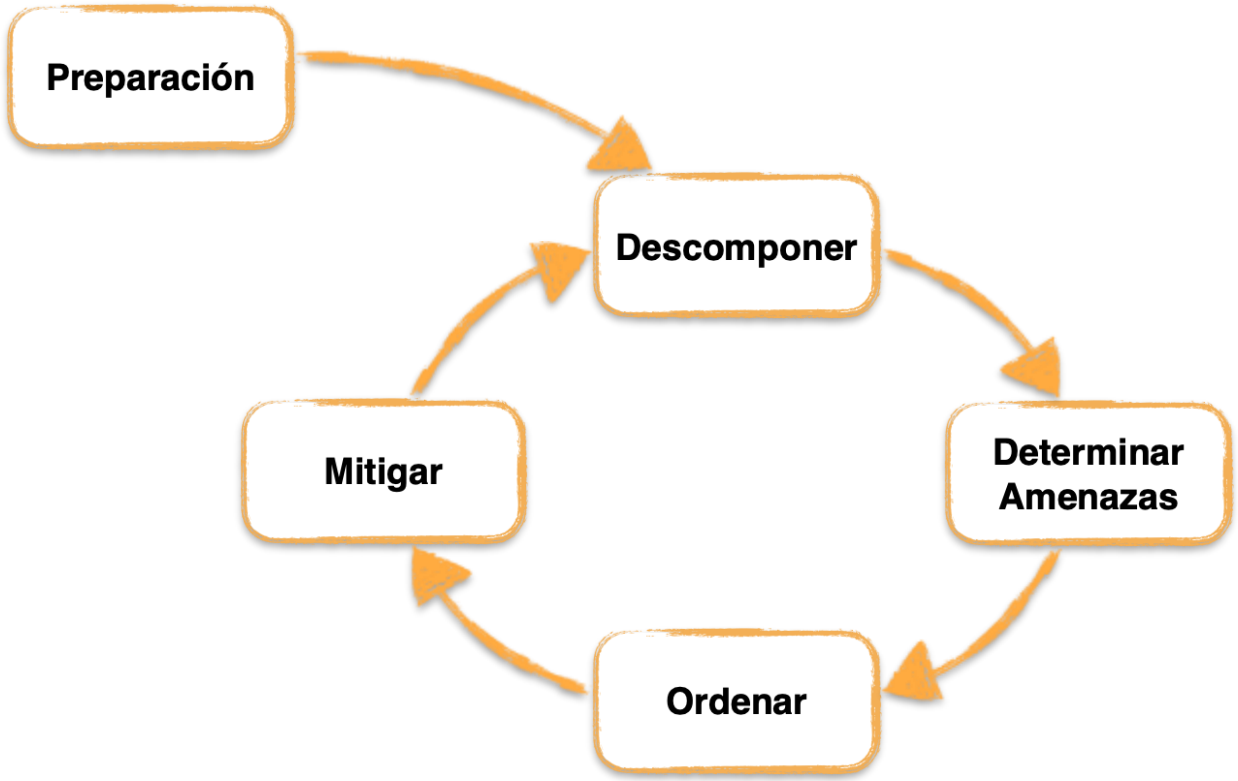
Características del Modelado de Amenazas

Proceso del Modelado de Amenazas

1. Composición equipo de desarrollo.
2. Descomposición de la aplicación.
3. Determinar y analizar amenazas.
4. Ordenar según riesgo decreciente.
5. Elegir estrategia de mitigación.

Características del Modelado de Amenazas

Proceso del Modelado de Amenazas



Composición equipo de desarrollo

Modelado de Amenazas

Unidad temática Nro. 4.2

Composición equipo de desarrollo

Composición

Es importante que alguien lidere el proceso de modelado.

- Es útil que sea la persona más hábil en temas de seguridad.
- Debe ser capaz de ver un sistema o componente y su contexto e idear cómo un atacante puede comprometerlo.
- Es más importante la experiencia en seguridad que en desarrollo - “El lado oscuro”.
- Es útil que haya más integrantes con experiencia en seguridad.

Composición equipo de desarrollo

Composición

- Es importante que esté al menos un representante de cada área.
- Análisis, diseño, codificación, testing, documentación, producción, seguridad, etc.
- Más perspectivas = visión más amplia de la realidad.
- Es útil invitar gente de marketing o ventas.
- Educa, y transmite directamente a los clientes los esfuerzos que se hacen para hacer el software seguro.

Composición equipo de desarrollo

Composición

- No sobrecargar el equipo.

Cuanta más gente, más probable es que se discuta con poco sentido.

- Documentar lo más que se pueda.
- Poner foco en empezar descomponiendo la aplicación e identificando la mayor cantidad de amenazas posibles.
- Las correcciones se hacen en reuniones posteriores.

Descomposición de la aplicación

Modelado de Amenazas

Unidad temática Nro. 4.3

Descomposición de la aplicación

“Pensar amenazas” es muy vago.

No estamos haciendo mucho para “ordenar el caos” a menos que vayamos un poco más allá.

Hay que “partir” la aplicación en componentes y analizar las interacciones para tener una visión más completa.

Descomposición de la aplicación

La descomposición debe ser ordenada, guiada por algún método formal, como UML.

- Diagramas de Componentes.
- Diagramas de Secuencia.
- Diagramas de Interacción.
- **Diagramas de Flujo de Datos (DFD).**

Diagrama de Flujos de Datos (DFD)

Modelado de Amenazas

Unidad temática Nro. 4.3.1

UCU

Diagrama de Flujos de Datos

Introducción

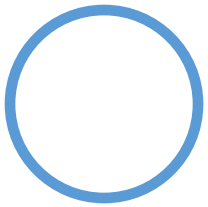
Un Diagrama de Flujo de Datos es una representación que modela los componentes de un sistema, junto con la manera en que los datos fluyen entre ellos.

Aunque se asemeja al diagrama de actividad de UML, este último se centra en el control de ejecución, mientras que el DFD se enfoca en las entradas y el intercambio de datos.

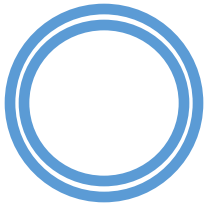
Este tipo de diagrama se caracteriza por ser 'atemporal', ya que no describe el inicio ni el fin de una actividad, sino que visualiza la ubicación potencial de los datos.

Diagrama de Flujos de Datos

Notación: Yourdon



Proceso: Manipula o procesa datos.

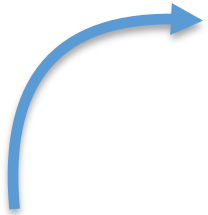


Proceso múltiple: Manipula o procesa datos.

Actor externo: ingresa y consume datos del sistema.

Almacén de datos (Data Store): Lugar donde se persisten datos.

Frontera: sistema, física, direccionamiento.



Flujo de datos: Entre Data Store, proceso, actor externo.

Diagrama de Flujos de Datos

Diagrama de Contexto - Primera Iteración

- En esta primera iteración, el objetivo es definir los límites y el alcance del sistema analizado. Esto implica la identificación de las partes confiables y no confiables del sistema.
- Normalmente, se comienza creando un diagrama que incluye un único proceso múltiple, las fronteras del sistema, los actores externos y los flujos de datos entre ellos.
- Posteriormente, en siguientes iteraciones, se procede a refinar este proceso múltiple en procesos atómicos, identificar los almacenes de datos y describir nuevos flujos de datos.

Diagrama de Flujos de Datos

Diagrama de Contexto (Ejemplo)

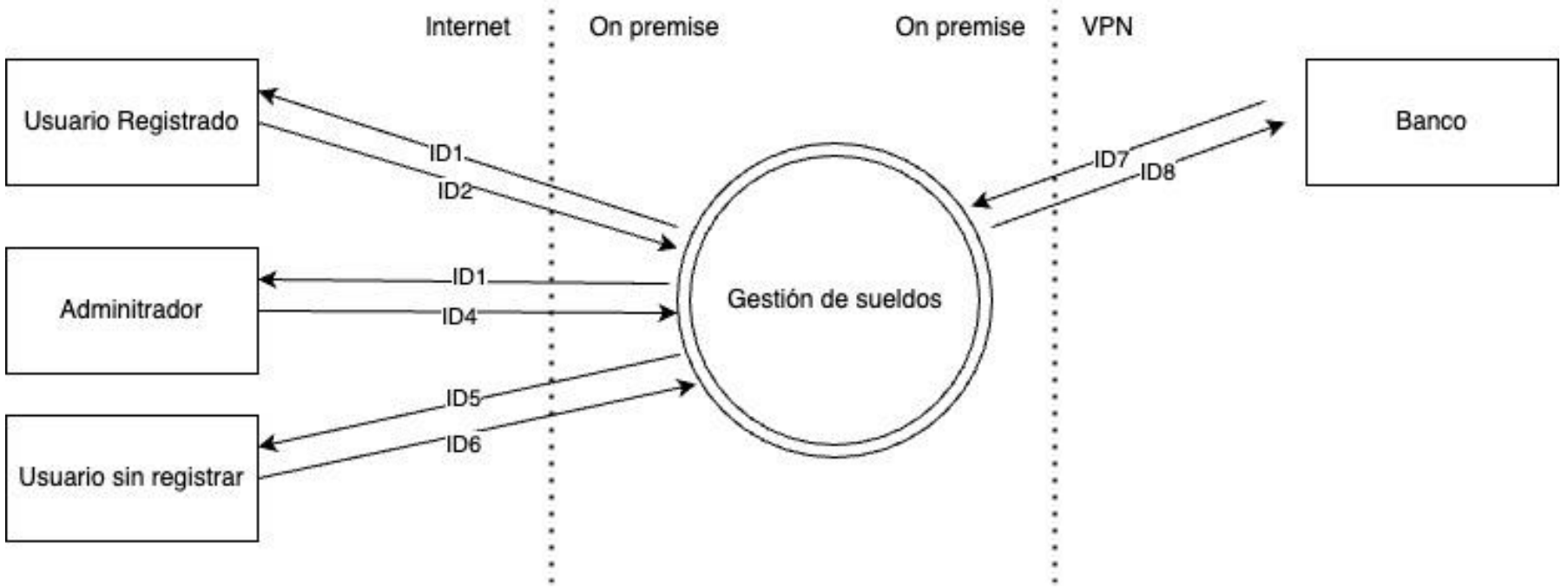


Diagrama de Contexto - Consejos

Cuando se trabaja en la creación de un Diagrama de Contexto, es importante seguir estos consejos:

- Ignorar los detalles internos de la aplicación cuando se busca el contexto general.
- Preguntarse a qué eventos debe responder el sistema.
- Considerar qué respuestas generará el sistema.
- Identificar las fuentes de datos en relación con las solicitudes (requests) y las respuestas (responses).
- Determinar que componente será el receptor de cada respuesta.

Diagrama de Flujos de Datos

Diagrama de Nivel Superior - Segunda Iteración

- En esta segunda iteración, el enfoque se centra en el refinamiento del proceso múltiple, la identificación de almacenes de datos (data stores) y la comprensión de los flujos de datos junto con sus interrelaciones.
- Este proceso se repite de manera iterativa hasta alcanzar un nivel de detalle que se considere aceptable.

Diagrama de Flujos de datos

Diagrama de Nivel Superior (Ejemplo)

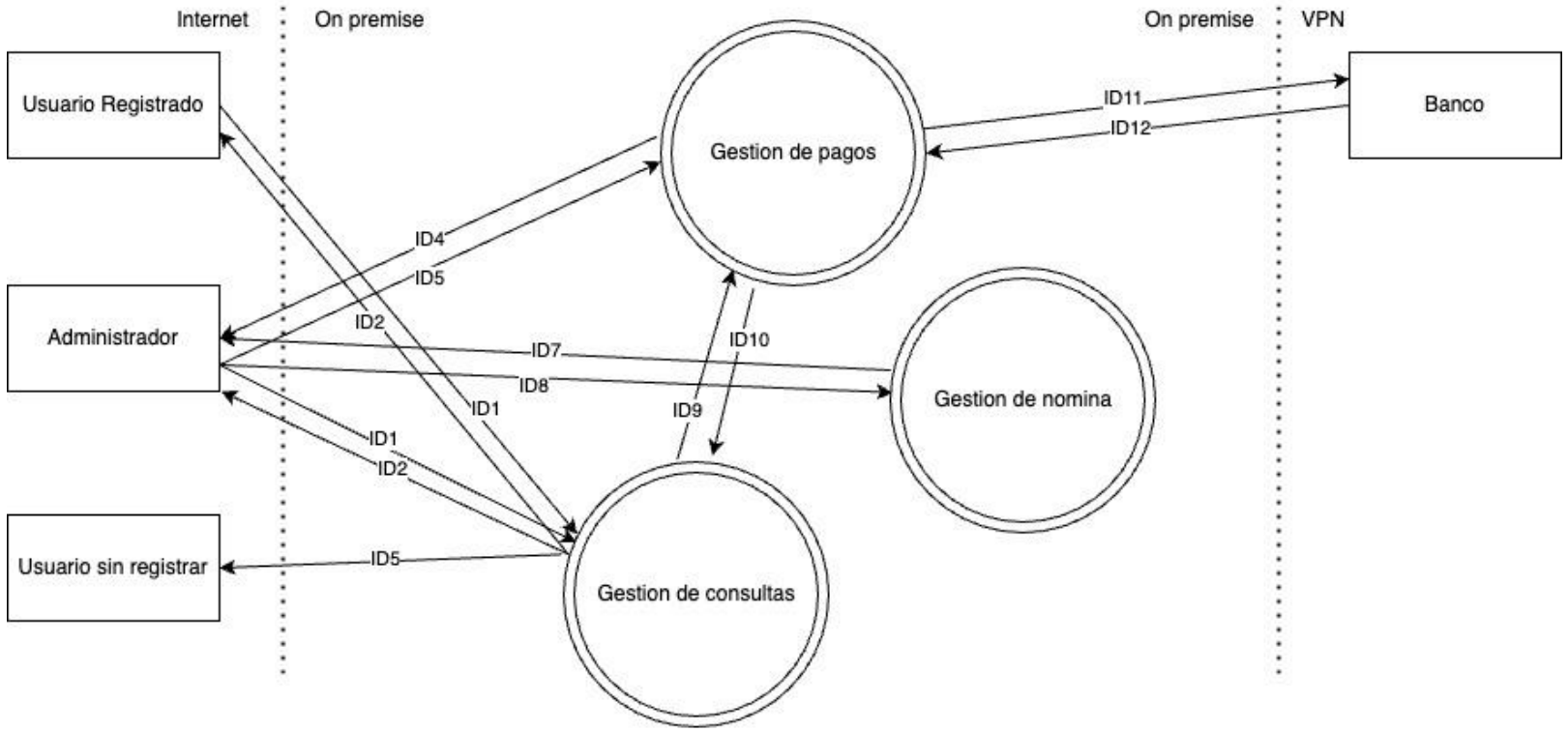


Diagrama de Flujos de Datos

Diagrama de Detalle o Expansión - Tercera Iteración

- En la tercera iteración, que suele ser suficiente para el Modelado de Amenazas, el enfoque no reside en diseñar el sistema en profundidad, sino en detectar problemas, que generalmente son de naturaleza externa.
- Es fundamental evitar caer en la parálisis y seguir avanzando con el proceso de identificación de amenazas y vulnerabilidades de manera efectiva.

Diagrama de Flujos de Datos

Conclusión del Diagrama de Detalle: Creación del Diagrama de Componentes

Para finalizar el proceso del Diagrama de Detalle, se parte del DFD más detallado. Utilizamos esta información para crear un Diagrama de Componentes o Implementación, en el cual identificamos los componentes tecnológicos que conformarán la arquitectura subyacente en la que se basará la aplicación.

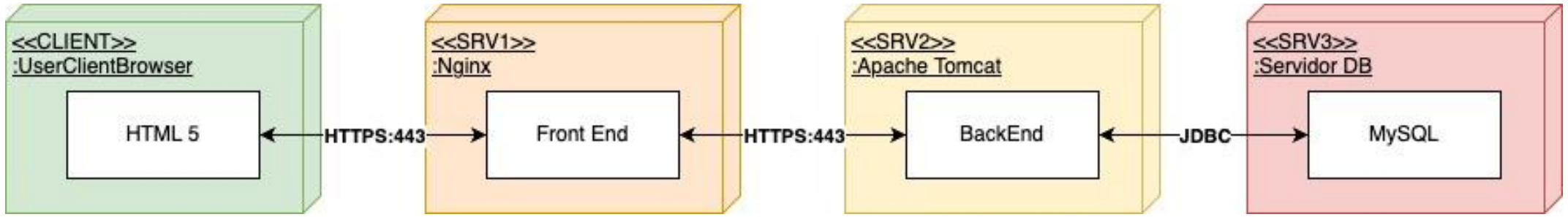


Diagrama de Flujos de Datos

Directrices para la Elaboración de un Diagrama de Flujo de Datos (DFD)

- **Cada proceso debe tener al menos un flujo de datos de entrada y uno de salida**: Esto asegura que cada proceso tenga conexiones definidas y claras tanto para recibir como para enviar datos.
- **Todos los flujos de datos deben tener un origen y un destino en un proceso:** Esto garantiza que cada dato tenga una fuente y un destino específico, evitando ambigüedades.
- **Los almacenes de datos se conectan a procesos a través de flujos de datos:** Esto refuerza la idea de que los procesos son los responsables de la manipulación de datos almacenados.

Diagrama de Flujos de Datos

Directrices para la Elaboración de un Diagrama de Flujo de Datos (DFD)

- **Los almacenes de datos no pueden conectarse directamente entre sí; un proceso debe estar entre ellos:** Esta regla mantiene la distinción clara entre los almacenes de datos y evita conexiones directas confusas entre ellos.
- **Los nombres de los procesos deben incluir un verbo y un sustantivo:** Esto ayuda a describir tanto la acción que realiza el proceso como el objeto en el que trabaja, lo que facilita la comprensión de su función.
- **Los nombres de los flujos de datos deben ser sustantivos:** Al nombrar los flujos de datos como sustantivos, se identifica claramente el tipo de datos que se está transfiriendo.

Diagrama de Flujos de Datos

Directrices para la Elaboración de un Diagrama de Flujo de Datos (DFD)

- **Los actores externos deben tener nombres que sean sustantivos:** Esto ayuda a identificar los roles de los actores externos en el sistema de manera más clara.
- **Los almacenes de datos deben tener nombres que sean sustantivos:** Similar a los flujos de datos y los teractores, los nombres de los almacenes de datos deben indicar claramente qué tipo de datos se almacenan en ellos.

Determinar y analizar amenazas

Modelado de Amenazas

Unidad temática Nro. 4.4

Determinar y analizar amenazas

Objetivo

- El objetivo del modelado anterior no es saber cómo funciona todo, sino realizar la identificación de los componentes y cómo fluyen los datos entre estos.
- A estos componentes se les llama Objetivos de Amenaza.

Determinar y analizar amenazas

¿Como abordar el análisis?

- Hay que mirar a cada componente y hacerse preguntas como:
- ¿Puede un usuario no autorizado (*UNA*) ver la información confidencial de la red?
- ¿Puede un *UNA* modificar registros en la BD?
- ¿Podría alguien evitar que usuarios válidos usen la aplicación?
- ¿Podría alguien usar un componente para obtener más permisos?

S.T.R.I.D.E.

Modelado de Amenazas

Unidad temática Nro. 4.4.1

UCU

S.T.R.I.D.E.

Modelo desarrollado por Praerit Garg y Loren Kohnfelder en Microsoft.

Provee una nemotecnia para seis categorías de amenazas:

- **S**poofing Identity
- **T**ampering with Data
- **R**epudiation
- **I**nformation Disclosure
- **D**enial of Service
- **E**levation of Privilege

S.T.R.I.D.E.

Spoofing Identity

Permiten a un atacante hacerse pasar por un usuario legítimo, o a un servidor malicioso hacerse pasar por uno legítimo.

- Phishing
- DNS Spoofing y DNS Caché Poisoning
- Rogue Access Points
- Ingresar un usuario de un tercero

S.T.R.I.D.E.

Tampering with Data

Modificación no autorizada de datos almacenados o en tránsito.

- Acceso no autorizado a base de datos
- ACL débiles
- Algún tipo de Man in the Middle
- Defacement
- Modificar datos que no deberían ser modificables

S.T.R.I.D.E.

Repudiation

Denegar acciones sin que la contraparte tenga posibilidades de probarlo.

- Falta de registros de auditoría adecuados.
- Falta de protección de registros de auditoría.
- Responde con evidencia a la afirmación: ¡Yo no lo hice!

S.T.R.I.D.E.

Information Disclosure

Pérdida de la confidencialidad. Revelar información a partes no autorizadas.

- Algún tipo de Man in the Middle.
- ACL débiles.
- Accesos a bases de datos.
- Criptografía débil o mal implementada.

S.T.R.I.D.E.

Denial of Service

Impedir que se brinde el servicio a usuarios legítimos.

- Consumir todos los recursos del servicio. (Ej. DDoS).
- Enumeración y bloqueo de cuentas de usuario.
- Defacement.

S.T.R.I.D.E.

Elevation of Privilege

Obtener mayores privilegios para un usuario limitado, que le permitan acciones administrativas sobre el sistema.

- Reescritura del shadow
- Plantar código malicioso
- Utilizar funciones de *administrador* siendo un usuario *común*

S.T.R.I.D.E.

- STRIDE ayuda a los equipos de desarrollo a organizar los impactos en los componentes.
- Frecuentemente, las amenazas están interconectadas.
- También es esencial considerar las causas de estos impactos.
- Este enfoque facilita la definición de estrategias de mitigación.

Árboles de ataque

Modelado de Amenazas

Unidad temática Nro. 4.4.2

Árboles de ataque

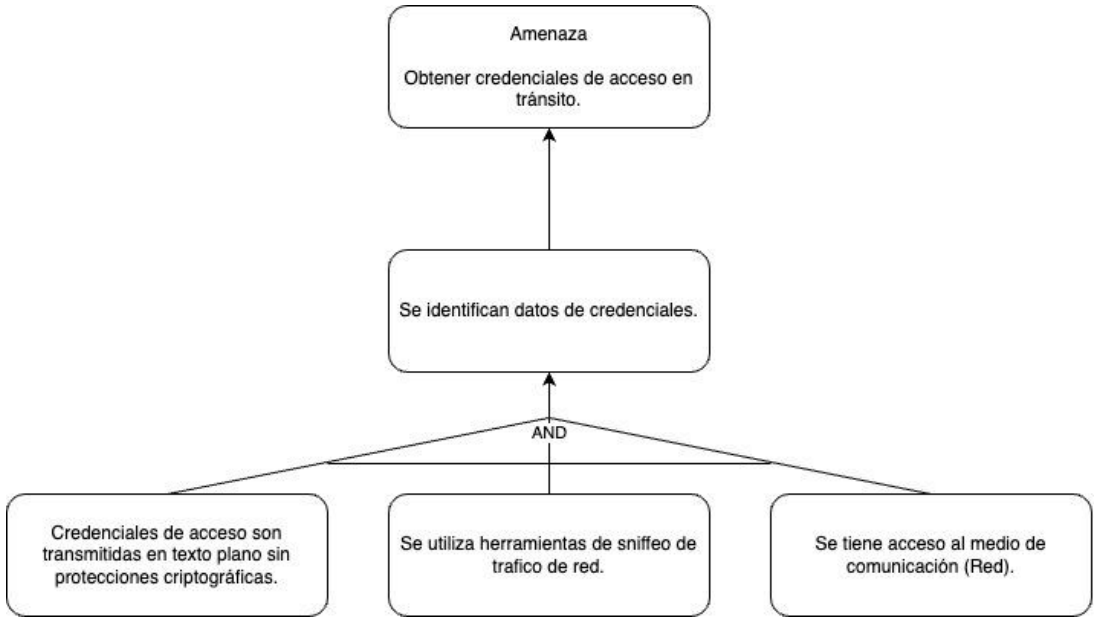
Contexto

- Una aplicación se compone de diferentes Objetivos de Ataque.
- Cada Objetivos de Ataque se asocia con vulnerabilidades que al ser explotadas pueden comprometer el sistema.
- El árbol de amenaza describe el proceso lógico del potencial ataque.

Árboles de ataque

AND

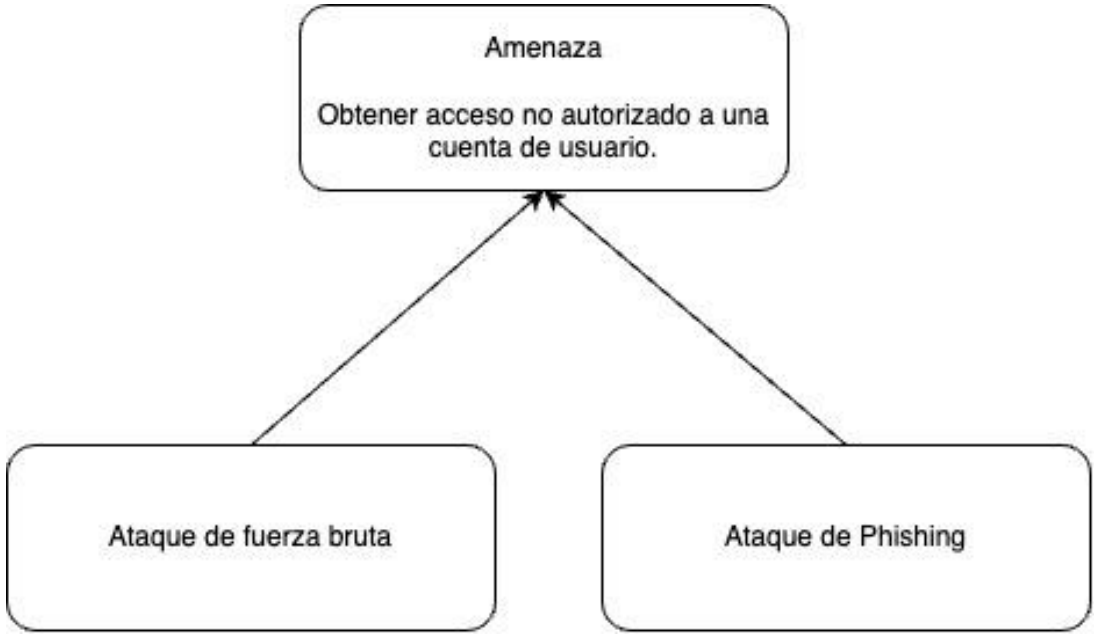
Existen al menos dos condiciones que se deben cumplir al mismo tiempo para materializar la amenaza.



Árboles de ataque

OR

Existen al menos dos condiciones que se pueden cumplir para materializar la amenaza.



Árboles de ataque

Documentación de amenazas

La identificación debe acompañarse de:

- Titulo.
- Objetivo de Ataque.
- Tipo(s) de Amenaza(s).
- Riesgo.
- Árbol de ataque.
- Técnicas de Mitigación.
- Estado de Mitigación (Si, No, Parcialmente, Req. Investigación).
- Número de defecto (Si se usa un bug tracker por ejemplo)

Evaluación y clasificación de riesgos

Modelado de Amenazas

Unidad temática Nro. 4.5

UCU

Evaluación y clasificación de riesgos

Cálculo de riesgo

Las amenazas identificadas deben ser prioridades y ordenadas según el valor del riesgo asociado a cada una de ellas.

El valor de riesgo se calcula típicamente como:

RIESGO = Probabilidad de Ocurrencia x Impacto

D.R.E.A.D.

Modelado de Amenazas

Unidad temática Nro. 4.5.1

D.R.E.A.D.

Contexto

Es un acrónimo utilizado para describir una metodología que permite evaluar y clasificar amenazas y riesgos en sistemas o aplicaciones.

- **D**amage (Daño)
- **R**eproducibility (Reproducibilidad)
- **E**xploitability (Explotabilidad)
- **A**ffected users (Usuarios afectados)
- **D**iscoverability (Detectabilidad)

D.R.E.A.D.

Damage (Daño)

- ¿Qué tanto daño puede hacer?
- 10 significa que elude todos los controles de seguridad y tiene control total.
- Elevation of Privilege.
- También se puede tomar en cuenta el impacto según el valor de la información o del sistema.

D.R.E.A.D.

Reproducibility (Reproducibilidad)

- ¿Qué tan reproducible es efectuar el ataque?
- 10 significa que funciona siempre.
- Cuestiones de configuración o versiones influyen en esta métrica.

D.R.E.A.D.

Exploitability (Explotabilidad)

- ¿Qué tanto esfuerzo y experiencia se requiere?
- 10 significa que un principiante con una PC de escritorio puede hacerlo.
- Exploits y Script-Kiddies.
- Requerir acceso a zonas seguras.
- 1 significa mucho conocimiento, esfuerzo y/o recursos
- Quebrar algoritmos criptográficos.

D.R.E.A.D.

Affected users (Usuarios afectados)

- Si se materializa un ataque, ¿cuánta gente se ve afectada?
- Se puntúa según el porcentaje de usuarios afectados.
- Tener en cuenta ataques al cliente o al servidor.
- Compartimentalización del riesgo.
- ¡No olvidar el volumen absoluto!

D.R.E.A.D.

Discoverability (Detectabilidad)

Qué tan probable/sencillo es descubrir la debilidad?

Si no se tiene una buena razón para no hacerlo, es sano asumir un puntaje de 10 para esta métrica.

Se asume que se encuentra fácil y luego las demás métricas hacen el ranking.

D.R.E.A.D.

Cálculo de riesgo

El puntaje se determina promediando los puntajes de todas las métricas.

El ordenamiento descendiente se hace sobre el puntaje D.R.E.A.D. para saber cuál es la más riesgosa.

Si lo aplicamos a los Árboles de Ataque, cada rama tiene un puntaje DREAD.

Hay que considerar a todas las amenazas, pero la amenaza raíz tiene como valor de riesgo el mismo que el máximo de sus ramas.

Estrategia de mitigación

Modelado de Amenazas

Unidad temática Nro. 4.6

Estrategia de mitigación

Selección de estrategia:

Generalmente tenemos 4 opciones de las cuales elegir:

- No hacer nada (asumir riesgo).
- Alertar al usuario.
- Eliminar el problema.
- Arreglar el problema.

Estrategia de mitigación

No hacer nada (asumir el riesgo)

Es una elección poco usual y es probable que al momento de identificar el problema se tenga que hacer algo de todas formas.

Puede afectar al negocio en el largo plazo.

Si se opta por esta opción, al menos intentar que la característica vulnerable esté desactivada por defecto.

Comúnmente este tipo de decisiones se toman de forma temporal, por ejemplo, por falta de recursos para aplicar una corrección.

Estrategia de mitigación

Alertar al usuario

- Puede ser usada cuando la necesidad del negocio es muy grande frente a un riesgo consciente, o el riesgo es muy bajo.
- Se debe intentar dejar desactivada por defecto, y presentar alerta al activar.
- Los usuarios, incluso expertos, tienden a ignorar las alertas (Lenguaje Técnico).

Estrategia de mitigación

Eliminar el problema

- Aplica cuando el costo o esfuerzo es demasiado grande para los deadlines.
- En lugar de no hacer nada o alertar, se saca la funcionalidad completa del producto.

Estrategia de mitigación

Corregir el problema

- Es casi siempre la opción más costosa.
- Entendido el riesgo de la amenaza y decidido que se va a arreglar, el siguiente paso es determinar qué tecnologías o técnicas de seguridad son adecuadas para hacerlo.

Finalización del modelado

Modelado de Amenazas

Unidad temática Nro. 4.7

UCU

Finalización del modelado

Finalizando el proceso

- El proceso de Modelado de Amenaza “termina” cuando para todas las amenazas identificadas de riesgo significativo se determinó una o varias técnicas y tecnologías de seguridad a aplicar.
- El resultado:
- Las técnicas y tecnologías de seguridad se aplican sobre las amenazas identificadas y siguiendo un método, lo cual es mejor que hacerlo en forma caótica.

Finalización del modelado

Resumen

1. Descomponer en objetivos de ataques usando D.F.D.
2. Aplicar S.T.R.I.D.E. para identificar y tipificar las amenazas.
3. Modelar los Árboles de Ataques para visualizar ataques complejos.
4. Utilizar D.R.E.A.D. para valorar los riesgos de las amenazas.
5. Ordenar y priorizar las amenazas de mayor a menor riesgo.
6. Seleccionar las estrategias de mitigación.

ucu.edu.uy