Perspectiva de seguridad

USAC - Análisis y diseño de sistemas 2 - 1er semestre 2016

Ing. Ricardo Morales

Detalles presentados para cada perspectiva

- Aplicabilidad a vistas
- Temas de interés mas importantes
- Descripción de actividades para aplicar la perspectiva
- Las tácticas clave de arquitectura a considerar
- Posibles problemas

Descripción

Calidad deseada

- La habilidad del sistema de controlar, monitorear y auditar confiablemente quien puede ejecutar acciones, que acciones sobre que recursos, y la habilidad para detectar y recuperarse de brechas de seguridad

Aplicabilidad

- Cualquier sistema con interfaces accesibles, con múltiples usuarios donde la identidad del usuario es significativa o donde el acceso a operaciones o información debe ser controlada

Descripción (II)

Temas de interés

- Recursos
- Principales
- Políticas
- Amenazas
- Confidencialidad
- Integridad
- Disponibilidad
- Auditabilidad
- Detección y recuperación
- Mecanismos de seguridad

Actividades

- Identificar recursos sensitivos
- Definir la política de seguridad
- Identificar amenazas al sistema
- Diseñar la implementación de seguridad
- Evaluar los riesgos de seguridad

Descripción (III)

Tácticas de arquitectura

- Aplicar principios reconocidos de seguridad
- Autenticar a los principales
- Autorizar acceso
- Asegurar el secreto de la información
- Asegurar la integridad de la información
- Asegurar la auditabilidad
- Proteger la disponibilidad
- Integrar tecnologías de seguridad

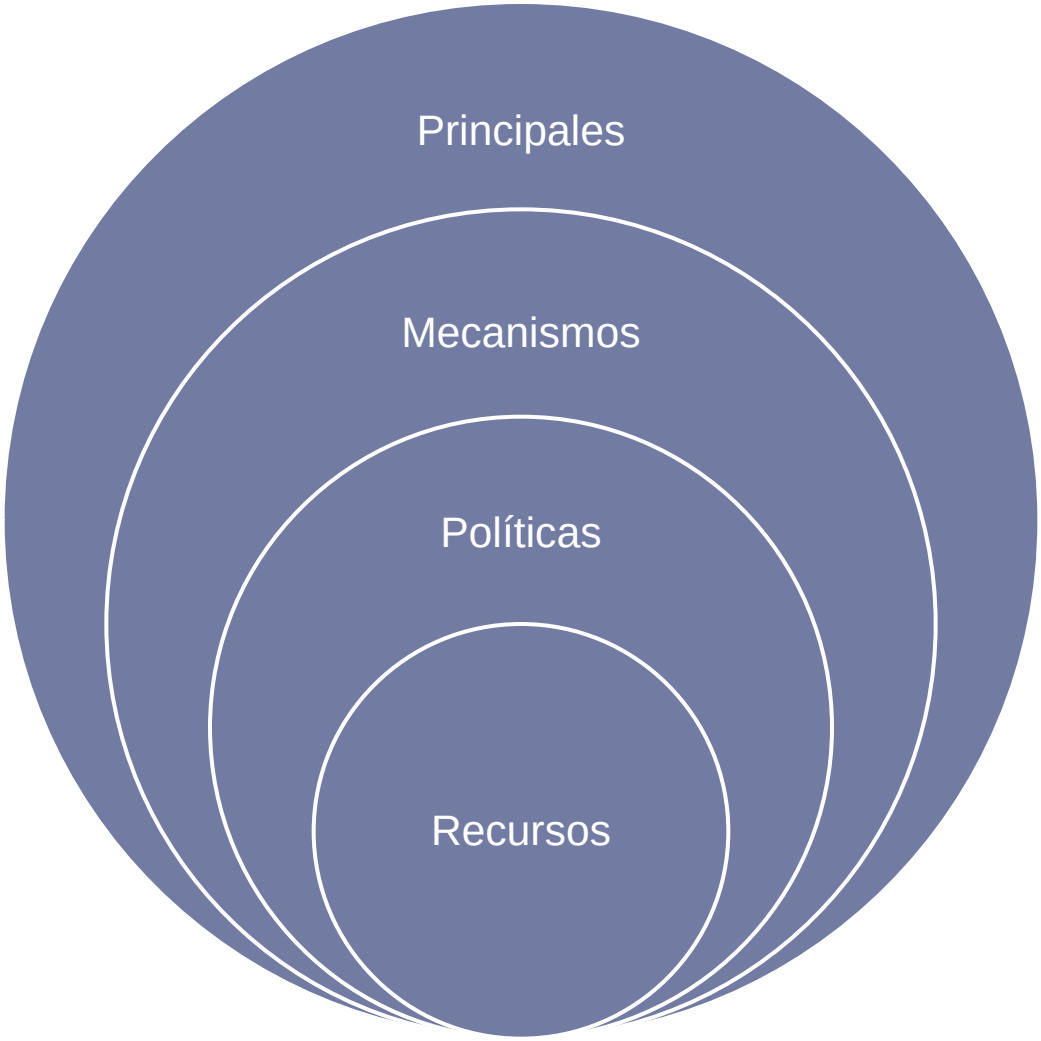
Problemas

- Políticas de seguridad complejas
- Tecnologías de seguridad no probadas
- Sistemas no diseñados para fallas
- Falta de facilidades para administración
- Mucha dependencia de tecnología
- Seguridad como algo secundario
- Ignorar amenazas internas

Descripción (IV)

- Seguridad se puede definir como el conjunto de procesos y tecnologías que permiten a los dueños de recursos en el sistema controlar confiablemente quienes pueden accesar dichos recursos
- El *quién* se refiere a personas, piezas de software, tienen una identidad de seguridad, se refiere normalmente a esos actores como *principales*
- Los *recursos* del sistema considerados sensitivos, como subsistemas, elementos de datos y operaciones
- Al *acceso* a esos recursos se refiere a las operaciones que los principales en el sistema ejecutar de forma legítima en los recursos
- Las *políticas* definen los accesos legítimos permitidos a los recursos, que son asegurados por *mecanismos de seguridad*

Descripción (IV)



Aplicabilidad a vistas

- La vista de contexto permite identificar claramente las conexiones externas del sistema y considerar como podrían convertirse en vulnerabilidades del sistema y como necesitarán ser protegidas de uso malicioso
- Es posible que al considerar la seguridad del sistema se llegue a cambiar la naturaleza de estas conexiones externas
- Esta vista también puede revelar posibles amenazas al sistema desde elementos en su ambiente inmediato

Contexto

- Permite ver claramente cuales elementos funcionales del sistema necesitan ser protegidos
- Adicionalmente, la estructura funcional del sistema podría ser impactada por la necesidad de implementar políticas de seguridad

Funcional

Aplicabilidad a vistas (II)

- Ayuda a ver que necesita ser protegido, en este caso, datos sensitivos en el sistema.
- El modelo de información es a menudo modificado como resultado de un diseño de seguridad (particionar información por grado de sensibilidad)

Información

- El diseño de seguridad debe indicar la necesidad de aislar diferentes piezas del sistema en diferentes elementos de ejecución, si es así, esto afectará la estructura de concurrencia del sistema

Concurrencia

Aplicabilidad a vistas (III)

Desarrollo

- Se pueden identificar guías o restricciones que los desarrolladores deban saber para asegurar que se cumpla la política de seguridad
- Es necesario incluir o referenciar estas guías o restricciones en la vista de desarrollo

Deployment

- El diseño de seguridad puede tener un impacto mayor en el ambiente de deployment del sistema
- Por ejemplo, puede se necesario hardware o software orientado a seguridad, que cambie lo que se había considerado

Operacional

- Cumplir la política de seguridad no es solo agregar factores tecnológicos a los sistemas
- Como se operará el sistema una vez esté en producción tendrá un efecto mayor en su seguridad

Temas de interés (concerns)

- Recursos
  - Los ítems en el sistema que se tratan de proteger son conocidos en la jerga de seguridad como recursos y la seguridad de computadoras es el negocio de diseñar procesos y mecanismos para proveer dicha protección
- Principales
  - Las entidades de nuestro sistema que necesitan ser identificadas por propósitos de seguridad son conocidos como principales
  - Puede ser una persona, rol, equipo físico u otro sistema
- Políticas
  - Definen las necesidades de seguridad del sistema
  - Define los controles y garantías que el sistema requiere para sus recursos e identifica que principales tendrán acceso y que tipo de acceso a cada recurso dentro del sistema

Temas de interés (II)

- Amenazas
  - Son las posibles formas en que las restricciones de seguridad pueden ser incumplidas por un atacante que quiere evadirlas
  - El considerar explícitamente las amenazas de seguridad al sistema permite identificar mecanismos que contrarresten dichas amenazas
  - Las amenazas mas comunes que los sistemas de información enfrentan son crackeo de passwords, ataques de red que exploten vulnerabilidades de configuración o software, ataques DoS, ataques de ingeniería social que buscan engañar a los usuarios para hacer operaciones en nombre del atacante
- Confidencialidad
  - Se define como limitar la revelación de secretos a aquellos que tienen permitido accesarlos de manera legítima
- Integridad
  - Es la garantía de que la información no pueda ser cambiada sin detectarse y asegurarse que la información no ha sido manipulada desde que fue creada o modificada por el principal

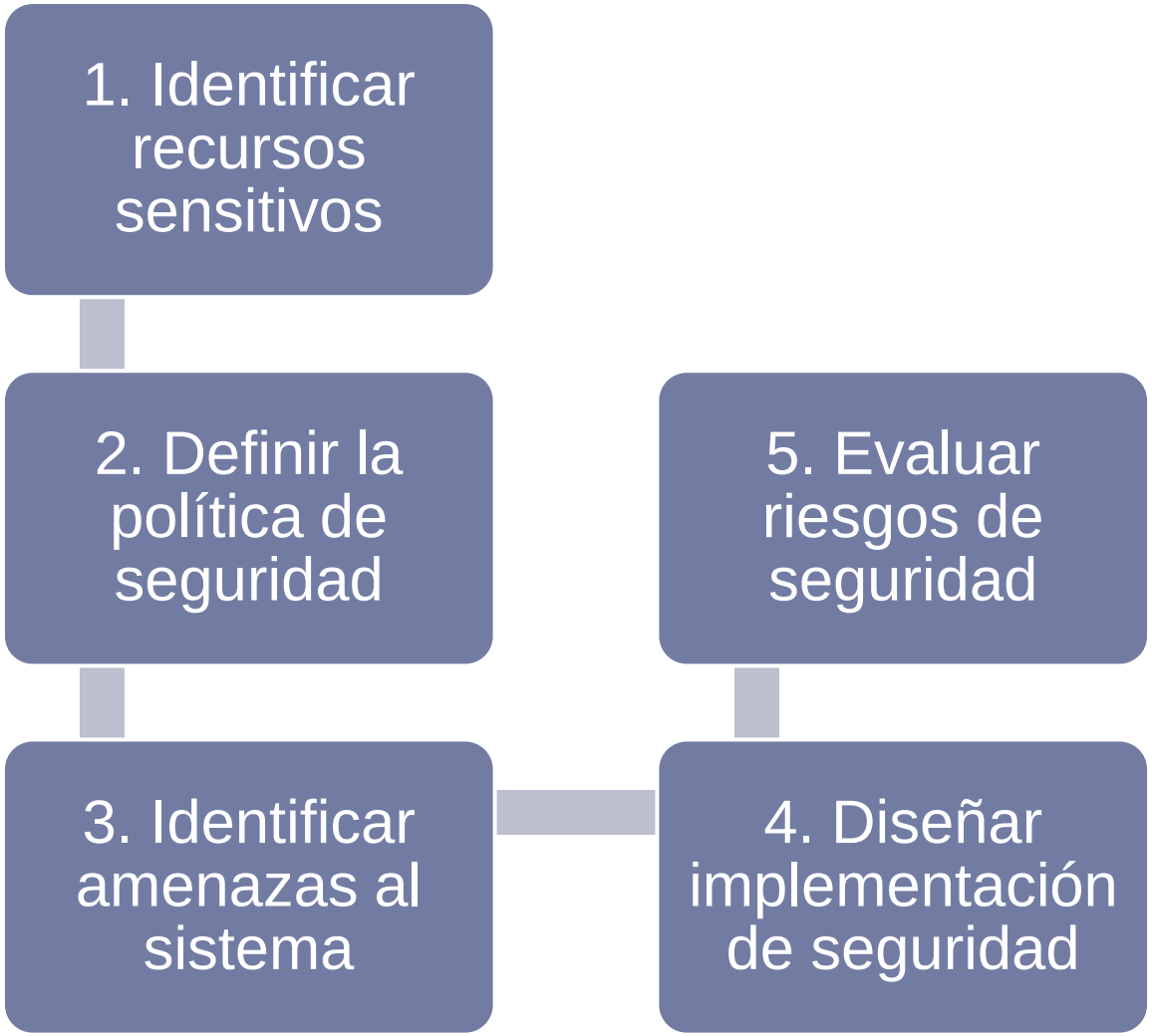
Temas de interés (III)

- Disponibilidad
  - Asegurar que atacantes potenciales no puedan bloquear la disponibilidad del sistema con ataques DoS es una parte importante del diseño de seguridad
- Auditabilidad
  - Es la forma de asegurar que cada acción pueda ser rastreada de forma no ambigua hacia el principal que la ejecutó
- Detección y recuperación
  - Habilidad del sistema para detectar brechas de seguridad y recuperarse de ellas

Temas de interés (IV)

- Mecanismos de seguridad
  - Los grupos de mecanismos son.
    - Autenticación, autorización y auditoría
    - Privacidad e integridad de la información
    - No repudiación
    - Disponibilidad del sistema
    - Monitoreo de seguridad

Actividades



Ejemplo de identificación de recursos sensitivos

Resource	Sensitivity	Owner	Access Control
Customer account records	Personal information of value for identity theft or invasion of privacy	Customer Care Group	No direct data access
Descriptive product catalog entries	Defines what is for sale and its description; if maliciously changed, could harm the business	Stock Management Group	No direct data access
Pricing product catalog entries	Defines pricing for catalog items; if maliciously or accidentally modified, could harm the business or allow fraud	Pricing Team in Stock Management Group	No direct data access
Business operations on customer account records	Needs to be controlled to protect data access and integrity	Customer Care Group	Access to individual record or all records by authenticated principal
Descriptive catalog operations	Needs to be controlled to protect data access and integrity	Stock Management Group	Access to catalog modification operations by authenticated principal
Pricing catalog modification operations	Needs to be controlled to protect data access and integrity	Pricing Team	Access to price modification operations by authenticated principal, with accountability of changes
. . .	. . .	. . .	. . .

Ejemplo de política de control de accesos

	User Account Records	Product Catalog Records	Pricing Records	User Account Operations	Product Catalog Operations	Price Change Operations
Data administrator	Full with audit	Full with audit	Full with audit	All with approval and audit	All with audit	All with approval from a product price administrator
Catalog clerk	None	None	None	All	Read-only operations	None
Catalog manager	None	None	None	Read-only operations with audit	All	All with audit
Product price administrator	None	None	None	None	Read-only operations	All with audit
Customer care clerk	None	None	None	All with audit	Read-only operations	None
Registered customer	None	None	None	All on own record	Read-only operations	None
Unknown Website user	None	None	None	None	Read-only operations	None

Ejemplo de evaluación de riesgos

Risk	Estimated Cost	Estimated Likelihood	Notional Cost
Attacker gains direct database access	$8,000,000	0.2%	$16,000
Web-site flaw allows free orders to be placed and fulfilled	$800,000	4.0%	$32,000
Social-engineering attack on a customer service representative results in hijacking of customer accounts	$4,000,000	1.5%	$60,000
. . .	. . .	. . .	. . .

Tácticas de arquitectura - Aplicar principios reconocidos de seguridad

- Algunos de los mas importantes principios son:
  - Otorgar la mínima cantidad de privilegios posibles
    - Dar el conjunto mas pequeño de privilegios necesarios para ejecutar una tarea
  - Asegurar el enlace mas débil
    - El enlace mas débil puede ser tecnológico (un enlace de red no asegurado), de procedimiento (permitir fácil acceso al data centro) o humano (personas que escriben sus claves en papel)
  - Defender en profundidad
    - En vez de depender de una medida de seguridad para contrarrestar amenazas, considere posibilidades de defensas en capas para proveer mayor protección
  - Separar y compartamentalizar
    - Buscar separar claramente responsabilidades diferentes de manera que la autoridad de cada una pueda ser asignada a diferentes principales si es requerido, y compartamentalizar responsabilidades para diferentes partes del sistema para que puedan ser controladas individualmente
  - Mantener el diseño de seguridad simple
    - La complejidad en un sistema es difícil de manejar y hace que el sistema sea difícil de analizar para evaluar la seguridad

Tácticas de arquitectura - Aplicar principios reconocidos de seguridad (II)

- Algunos de los mas importantes principios son:
  - No depender de la obscuridad
    - En lugar de depender de ocultar medidas de seguridad, se recomienda que dichas medidas sean conocidas internamente para evaluarlas
  - Usar valores por defecto seguros
    - Se refiere a configurar comportamiento y configuración por defecto que sea segura, como claves y puertos abiertos
  - Fallar seguramente
    - Se debe verificar que cuando el sistema falle, las medidas de seguridad no dejen de funcionar
  - Asumir que las entidades externas no son confiables
  - Auditar eventos sensitivos

Tácticas de arquitectura

- Autenticar a los principales
  - Autenticación es la identificación confiable de los principales que pueden usar el sistema
  - Existen varias tecnologías como nombre de usuario y clave, sistemas de llaves públicas/privadas y tecnologías de tokens de hardware
  - Lo que es crítico a nivel de arquitectura es que cada principal pueda ser autenticado cuando se requiera y que el sistema usado sea simple y usable
- Autorizar acceso
  - Un problema clave para la arquitectura es como crear un sistema coherente de control de accesos, partiendo de que pueden existir varias tecnologías para autenticar y autorizar
  - Una solución es utilizar un producto para manejar el control de accesos, que interactúa con varios sistemas de autenticación
  - Otro enfoque común es estandarizar el chequeo de autorización contra un directorio empresarial (LDAP)

Tácticas de arquitectura (II)

- Asegurar el secreto de la información
  - El secreto puede ser parcialmente alcanzado a través de un uso apropiado de la autorización, aunque generalmente no es suficiente
  - La distribución de información en varios equipos complica este escenario
  - La criptografía es una opción a utilizar, pero tiene un costo, tanto financiero como de procesamiento
  - En general, se debe usar el modelo de amenazas para identificar donde se debe proteger la información y usar el nivel mínimo de criptografía necesario
- Asegurar la integridad de la información
  - Es asegurar que la información está protegida de cambios no autorizados, generalmente durante la transmisión
  - Generalmente involucra el uso de criptografía
- Asegurar la auditabilidad
  - Tienden a existir 2 formas de auditabilidad, auditoría y no repudiación de mensajes
  - Auditoría es el manejo de logs cuando se utilizan servidores centralizados para el procesamiento, tiene impacto en el rendimiento
  - En sistemas distribuidos el análogo a la auditoría es la no repudiación, la habilidad de identificar al creador de un mensaje de manera que no se pueda negar, en este caso se debe considerar el costo de generar y administrar firmas digitales

Tácticas de arquitectura (III)

- Proteger la disponibilidad
  - Al pensar en disponibilidad es natural enfocarse en confiabilidad del software, replicación de software, failover, etc., pero no se consideran ataques DoS
  - Se debe evaluar las amenazas para determinar costos y riesgos, para definir estrategias
- Integrar tecnologías de seguridad
  - Generalmente se necesitará diferentes tecnologías para el tema de seguridad, parte del diseño debe considerar como se integrarán
- Proveer administración de seguridad
  - Como parte de la definición de arquitectura se debe asegurar que la implementación planeada de seguridad pueda ser administrada adecuadamente