Metodología Rational Unified Process-Secure (RUPSec)

Integrantes:

Jonathan García

Axel Herrera

Bryan Quispe

Índice

Introducción

extensión de seguridad del Rational Unified Process (RUP) de IBM, la cual se enfoca en ser iterativa e incremental, incorporando actividades de seguridad, roles y artefactos en cada iteración, en lugar de tratar la seguridad como una etapa final del ciclo de vida. Su objetivo es integrar la seguridad como una disciplina dentro del proyecto

Objetivos

- Según la metodología de Rational Unified Process-Secure (RUPSec) se debe describir, enumerar las etapas del ciclo de vida y herramientas recomendadas para cada etapa.
- Especificar ventajas y desventajas de su implementacion con casos de uso o ejemplos reales
- Analizar cómo la integración de prácticas de seguridad en cada fase del RUPSec contribuye a la prevención temprana de vulnerabilidades y al fortalecimiento del producto final.

Descripcion General

Process-Secure (RUPSec) es una adaptación del Proceso Unificado Rational (RUP) que incorpora prácticas de seguridad en cada fase del ciclo de desarrollo. Su objetivo es integrar análisis de riesgos, requisitos de seguridad, diseño seguro, pruebas de seguridad y revisiones continuas, de modo que el software se construya con protección desde el inicio y no como un añadido final.

Seguridad a través de las Fases (Ciclo de Vida)

1. **Inicio (Inception):** Identificación de requisitos de seguridad y riesgos críticos.

2. **Elaboración (Elaboration):** Diseño de arquitectura segura y Modelado de Amenazas.

3. **Construcción (Construction):** Codificación segura y pruebas unitarias de seguridad.

4. **Transición (Transition):** Auditorías finales, Pen-testing y despliegue seguro.

Herramientas y Prácticas

Modelado de Amenazas

- Anticipar ataques antes de programar

Microsoft Threat Modeling Tool

Revisión de Código

- Peers revisando posibles vulnerabilidades.

Análisis Estático (SAST): SonarQube, Fortify (Revisan el código sin ejecutarlo).
Análisis Dinámico (DAST): OWASP ZAP, Burp Suite (Atacan la app funcionando)

Defensa en Profundidad

- Múltiples capas de seguridad

WAF (Web Application Firewall) : Filtran el tráfico malicioso antes de que toque tu código EJM ModSecurity

Gestores de Secretos (Secrets Management): En lugar de guardar contraseñas en el código, se usan bóvedas digitales Ejm. HashiCorp Vault

Gestión de Identidades (IAM): Herramientas que aseguran que quien entra es quien dice ser (MFA, autenticación fuerte Ejm. Keycloak

Caso Real Gubernamental: Web Service Seguro

Introducción

El sistema real consistió en un web service utilizado para compartir información sensible entre varias instituciones públicas.
Los riesgos asociados incluían fuga de datos personales, manipulación de consultas, accesos no autorizados y falta de trazabilidad.
Los requisitos de seguridad definidos fueron: autenticación fuerte mediante certificados, cifrado extremo a extremo, auditoría obligatoria, validación estricta de mensajes y registro detallado de eventos.

Elaboración

El equipo realizó un modelado de amenazas, identificando riesgos externos, internos y técnicos.

La arquitectura se diseñó con múltiples capas:

- VPN interinstitucional,
- Firewalls segmentados e IDS,
- WS-Security,
- Validación de esquemas XSD,
- Cifrado AES-256 en base de datos,
- Controles RBAC por institución,
- Logs inmutables enviados a un SIEM.

Construcción

Se aplicaron revisiones formales de código según normas de seguridad del Estado, junto con análisis automatizado mediante Fortify y Veracode.

Las pruebas incluyeron:

- Pruebas de penetración internas,
- Evaluación contra inyección XML (XXE),
- Fuzzing de endpoints SOAP/REST,
- Simulación de ataques replay.

Transición

El sistema fue desplegado bajo un proceso de certificación de seguridad. Se implementó monitoreo 24/7, rotación de certificados, controles estrictos de acceso y auditorías semestrales.

La trazabilidad se mantuvo en todas las etapas: desde requisitos hasta pruebas y cambios en producción, asegurando cumplimiento normativo.

Conclusión

El caso demuestra la aplicabilidad de RUPSec en un entorno critico. Esta metodología permite un enfoque ordenado, iterativo y auditable, integrando seguridad desde las primeras etapas y manteniéndola durante todo el ciclo de vida. Esta plataforma gubernamental se beneficia de RUPSec al enfrentar riesgos elevados, cumplir regulaciones y asegurar la continuidad operativa.

Thank You