Relevamiento de Seguridad

En la clase del miércoles 26 de mayo, el profesor Tomasini habló sobre los requerimientos de seguridad.

Él definió dos tipos de seguridades:

1. **Seguridad funcional**

Habla de “usuarios” y “roles”, donde a cada usuario se le pueden asignar determinados roles. Esta asignación puede estar implementada como:

* + Habilitación de permisos
  + Denegación de permisos
  + Asignación específica de un permiso
  + Denegación específica de un permiso

1. **Seguridad objetos (o “por valor”)**

Se explica con un ejemplo: “Una empresa tiene sucursales y una sede central. En la sede central está el administrador y él dispone de los accesos y roles al resto de las sucursales. Entonces, de esta manera se puede asignar determinado acceso a la sucursal XI, por ejemplo”.

Es importante destacar que debe ser “on line”. Es decir, que los cambios deben aplicarse sobre el usuario sin la necesidad de salir e ingresar al sistema nuevamente (no pocas palabras, no debe hacerse login/logout para ver los cambios).

Administrador de Seguridad. Toda modificación de permisos debe hacerse con una interfaz.

Los siguientes ejemplos son modelos de evaluación que ejecutarán los profesores el día de la presentación del mismo.

Ejemplo 1

* Cargar un usuario (o tomar uno existente)
* Crear un rol (o tomar uno existente)
* Asignar esos roles a un usuario
* Crear agrupación de permisos
* Crear objetos del sistema (métodos de un objeto en particular, acciones)
* Tiene que ser posible expresar los permisos o restricciones en forma de regla de seguridad: “Determinado atributo debe tener valores positivos”.

Ejemplo 2

* Establecer un Rol
* Darle acceso a un determinada funcionalidad (o acción)
* Evaluar si el usuario puede acceder o no.

Ejemplos de Reglas restrictivas para Reserbar

* “Un restaurante puede definir el horario de rangos horarios en que quiere tomar reservas”.
* “Un restaurante puede definir el *deadline* previo a la hora de reserva” (deadline: tiempo previo a la ejecución de la reserva).
* “Se puede crear un segundo *deadline* en el caso de reservas grandes”

Definición de producto, según Tomasini:

Producto: Es un objeto genérico, donde se puede personalizar (parametrizar) características al momento de la instalación y que luego esos valores quedan estables.

Otras particularidades

Entregables

* Manual de instalación
* Manual de usuario
* Manual de administrador

En el plan de calidad debe haber definido una política similar a: “nosotros no testeamos más cuando la probabilidad de error es menor a %30”

Esto lo nombró, pero supongo que no es obligatorio:

“Cómo es el estándar de presentación de pantallas”

Al momento de presentar el trabajo final, debemos mostrar los resultados de analizar la información:

* Mostrar las estimaciones vs lo real.
* Gaps (tiempos muertos que se producen por estar una tarea dependiente de la otra, etc.)
* Dónde nos chocamos con problemas
* Problemas con la arquitectura, problemas con el uso de determinada herramienta.
* Cálculo de costos
* Informes de impacto (qué requerimientos tocó y afectó)
* Demostrar mantenibilidad del sistema