Unidad IV: Seguridad en Ingeniería de Software

La seguridad de software aplica los principios de la seguridad de informació n al desarrollo de software. Information security (La seguridad de información) se refiere a la seguridad de información comúnmente como la protección de sistemas de información contra el acceso desautoriza do o la modificación de información, si está en una fase de almacenamiento, procesamiento o tránsito.

También la protege contra la negación de servicios a usuarios desautorizados y la provisión de servicio a usuarios desautorizados, incluyendo las medidas necesarias para detectar, documentar, y contrarear tales amenazas.

Muchas preguntas con respecto a la seguridad, son relacionadas al ciclo vital de software. En particular, la seguridad del código y el proceso de software; deben de ser considerados durante la fase del diseño y desarrollo. Además, la seguridad debe de ser preservada durante la operación y el mantenimiento para asegurar la integridad de una parte (pedazo) de software.

Una gran cantidad de seguridad usada en los Sistemas de Redes de hoy, nos pueden engañar en lacreencia que nuestros trabajos como diseñadores de sistema de seguridad ya han sido realizados. Sin embargo, las cadenas y computadoras son increíblemente inseguras. La falta de seguridad se origina en dos problemas fundamentales: Los sistemas que son teóricamente seguros p ueden ser inseguros en lapráctica, Además los sistemas son cada vez más complejos. La complejidad proporciona más oportunidades para los ataques. Es mucho más fácil probar que un sistema es inseguro que demostrar que uno es seguro probar la inseguridad, simplemente una toma ventaja de ciert as vulnerabilidades del sistema.

4.1 Seguridad de software

El concepto de la seguridad en los sistemas de software es un área de investigación que ha pasado a ser vital dentro de la Ingeniería de Software. Con el

crecimiento de Internet, y otras aplicaciones sobre redes, como el comercio electrónico, correo electrónico, etc., la posibilidad de ataques se ha incrementado notablemente, como también lo han hecho las consecuencias negativas de estos ataques.

En la actualidad prácticamente todo sistema debe incorporar cuestiones de seguridad para defenderse de ataques maliciosos. El desarrollador ya no sólo debe concentrarse únicamente en los usuarios y sus requerimientos, sino también en los posibles atacantes.

4.2 Seguridad en el ciclo de desarrollo del software

La mayor parte de las organizaciones desarrolla o contrata el desarrollo de aplicaciones propias para su gestión de negocio. Como todo software, estas aplicaciones pueden contener fallas de seguridad y a diferencia del software comercial, no se dispone de actualizaciones o parches liberados en forma periódica por el fabricante. El tratamiento de las vulnerabilidades en aplicaciones propias corre por parte de la organización que las desarrolla.

Lamentablemente es una práctica habitual en muchas organizaciones la “puesta en producción” de sistemas sin la participación del sector de Seguridad de la Información.

Muchas otras veces, el sector de Seguridad se entera demasiado tarde, y no tiene suficiente margen de acción para el análisis de seguridad de la aplicación desarrollada.

Por lo general, en el mejor de los casos, se coordina un testeo de seguridad una vez que la aplicación ya está desarrollada. Aquí muchas veces se encuentran errores que requieren el rediseño de parte de la aplicación, lo cual implica un costo adicional en tiempo y esfuerzo.

4.3 Confiabilidad del software

La confiabilidad de software significa que un programa particular debe de seguir funcionando en la presencia de errores. Los errores pueden ser relacionados al diseño, a la implementación, a la programación, o el uso de errores.

Así como los sistemas llegan a ser cada vez más complejos, aumenta la probabilidad de errores.

Como mencionamos, es increíblemente difícil demonstrar que un sistema sea seguro. Ross Anderson dice que la seguridad de computación es como programar la computadora del Satán. Software seguro debe de funcionar abajo de un ataque.

Aunque casi todo el software tenga errores, la mayoría de los errores nunca serán revelados debajo de circunstancias normales. Un atacante busca esta debilidad para atacar un sistema.

Las organizaciones que desarrollan productos basados en software requieren de prácticas efectivas que permitan mejorar la calidad del producto. La Ingeniería de la Confiabilidad de Software es una práctica cuantitativa que puede ser implementada en organizaciones de cualquier tamaño bajo distintos modelos de desarrollo.

Las organizaciones desarrolladoras de productos basados en software destinan grandes cantidades de recursos para mejorar la calidad de sus productos. Una parte de dichos recursos se utiliza para la adopción de mejores prácticas. Sin embargo, la dificultad de la adopción de dichas prácticas no sólo reside en el costo y el tiempo requerido para institucionalizarlas, sino en cómo medir su impacto en la calidad del software, así como demostrar el retorno de dicha inversión.

La calidad, las fallas y la confiabilidad de Software

La calidad es un atributo percibido por los usuarios o clientes de cualquier producto o servicio. En el caso de productos basados en software, la percepción de la calidad está en función de las fallas que el cliente percibe del mismo durante su operación.

La confiabilidad es un atributo que mide el grado en que un producto opera sin fallas bajo condiciones establecidas por un periodo de tiempo determinado. La confiabilidad es un atributo cuantitativo que ha sido ampliamente analizado, estudiado y usado en otras industrias para caracterizar la calidad de los productos o servicios.

En su concepción más general, la confiabilidad es un atributo que mide el grado en que un producto opera sin fallas bajo condiciones establecidas por un periodo de tiempo determinado.

Una falla es la manifestación percibida por el cliente de que algo no funciona correctamente e impacta su percepción de la calidad. Un defecto es el problema en el producto de software que genera una falla.

4.4 Ingeniería de seguridad

La Ingeniería de la seguridad es una rama de la ingeniería, que usa todo tipo de ciencias para desarrollar los procesos y diseños en cuanto a las características de seguridad, controles y sistemas de seguridad. La principal motivación de esta ingeniería ha de ser el dar soporte de tal manera que impidan comportamientos malintencionados.

Tradicionalmente el tema de la seguridad en sistemas computarizados se ha asociado a la criptografía y sus técnicas. La inmensa complejidad que caracteriza a los sistemas modernos hace que esta aproximación sea insuficiente.

Hoy en día la seguridad está asociada a la interacción de una multiplicidad de sistemas. La seguridad de un sistema en particular está directamente relacionada a la seguridad de la más débil de sus partes.

Un sistema puede tener mecanismos criptográficos que sean considerados completamente seguros pero puede adolecer de debilidades que hagan que sea innecesario atacar al sistema criptográfico.