EfectivoModelado de amenazas – Uso de TAM

En mi [blog entry](http://blogs.msdn.com/ace_team/archive/2007/05/01/threat-modeling-sanity-check-list.aspx)con respecto a:**T**hreat**A**nalysis y**M**herramienta de odeling (TAM) desarrollado por(**A**pplication**C**de la OBLIGACIÓN Y**E**ngineering)ACE,He visto muchos más modelos de amenaza que se construyen para marcar una casilla en eldesarrollolista de verificación o fueron intentos sinceros de entender el perfil de amenaza de la aplicación. La mayoría de ellos fueronizquierda queriendo mucho másque eraproducidos.

Retrocede un poco,vamos eche un vistazo a la historia de la herramienta TAM.

El equipo de ACE lanzó el código de herramienta Threat Modeling llamado Torpedo internamente para(Microsoft)MS en 2004. Esto era v1.0 que iba a ser utilizado para toda la aplicaciónlas condiciones de acceso a la información y a la información;desarrollado para la tecnología de la información de los Estados miembros(MicrosoftTecnología de la información). Más de 600 TM s fueron creados utilizando esta versión, pero debido a que sus usuarios objetivo eran expertos en seguridad pronto no había suficientes expertos para sacar los TM s a la velocidad requerida. Esta versión fue muy útil para encontrar muchos problemas de diseño con aplicaciones internas de MS, pero el gran tamaño de las operaciones y la falta de suficientes expertos en seguridad exigió otra mirada a la situación.

La metodología y la herramienta V2.0 se crearon para simplificar la terminología, y la metodología más fácil, aspecto y sensación renovados fueron algunos de los aspectos más destacados de la versión v2.0.Versión2.0 fue lanzado para que la gente descargara en el[MSDN](http://msdn2.microsoft.com/)(Microsoft Developer Network)sitio en 2005. Después de la primera versión ha habido un interés creciente continuo en la herramienta TAM y cada vez más personas dentro de MS, así como clientes externos comenzaron a utilizar TAM.Esto también fue un gran hito para[ACE Services](http://blogs.msdn.com/ace_team);ya que estaba disponiblegratis [download](http://msdn2.microsoft.com/en-us/security/aa570413.aspx). Esta exposición a un consumo más amplio dio lugar a que los clientes que desean formación y más material a su alrededor. Ford y Boeing son algunos de los clientes externos que actualmente están utilizando TAM v2.0 en sus procesos internos de SDLC.

Estas mejoras han ayudado a construirmuchodeconciencia alrededor de TAM. Me he encontrado con practicantes de varias disciplinas que quieren empezar a hacer modelos de amenazaspara conseguir unvista dela posible amenazasa su sistema.Para empezar,el modelo de amenaza utilizando TAM parece seraproceso muy simple y directo hacia adelantederecho desdedescargando la herramientapara producir una característica rico modelo de amenaza.Este proceso aparentemente simple y eficaz merece cierta atención.y la debida diligencia en el ordenpara construiruna buenamodelo de amenaza.Algunas de las consideracionespara un modelo eficaz de amenazasson los siguientes:

1. Es de vital importancia tener acceso a las personas y a la información relativa a todos los aspectos de la aplicación. allí.es unasignificativaparticipación de personal no técnico en el proceso.
   1. El proceso de TM comienza con la captura de las necesidades del negociosu objetivosde la solicitud ycontinúaa través deladesarrollo y desarrollofase de mantenimiento de la aplicación.Mantener el modelo de amenaza se convierte en una parte continua de la vida útil de la aplicación para dar cuenta de las amenazas nuevas y emergentesy ataques. Sin embargo, la mayor parte del trabajo de TM se realiza en las primeras etapas de desarrollo, antes de que se escriba cualquier código. Esto proporciona un enfoque proactivo fuertea construcción de software seguro y evita costosas reparaciones debido a la seguridad retro-fittingNecesidades cuando los fallos de seguridad se descubren tarde en el proceso.Por lo tanto, el proceso de TM requierebuscar información de las empresaspropietariosaayudarCategoríaze, y rangolas amenazas identificadas.
   2. La mayoría de los propietarios de negocios que patrocinan el desarrollo de aplicaciones tienen muy poco tiempo a la mano;así que para conseguir una ranura en su horario ocupado uno necesita tener buenarelacionescon personas que “importan”.Esta participación ayuda al grupo técnico a traducir el riesgo técnico en impacto empresarial, lo que proporciona una mayor comprensiónen ellos niveles de negocio para que apoyen el proceso.
2. Utilizar principios de seguridad como el uso de menos privilegios, la reducción de la superficie, etc. para verificar supuestos e información según lo proporcionado por el equipo
   1. Ciertas categorías de amenazas no son directamente evidentes, como por ejemplo:enforcingo bien las cuentas de servicio o las cuentas de usuario con menos privilegios para invocar el código. Esto puede dar lugar a usuarios o servicios,que, en caso de compromiso,,exponer mucho más que sólo el código de aplicación y los datos al atacante.TAM demuestra ser una herramienta muy poderosa en tal situación al proporcionarnos una matriz de control de acceso de datos. Esta representación única permite a los arquitectos de bases de datos y arquitectos de aplicaciones garantizar que no hay acceso no autorizado a los datos.
   2. Proporciona una manera de identificar muy explícitamente el acceso y los privilegios que las funciones necesitan.tcualquier otro derecho yprivilegios quelos descritos en el Data ACM.

Figura1: DataAccesoControlMatrix

* 1. Para la reducción de la superficie de ataque la“...............................................................................................................análisis de superficie de ataque”herramienta será de gran ayuda.Esto ayudará.¿Entiendes?diversas formas en que cualquier componente en particular podría# Ser # # Ser # # Ser # # Ser # # Ser # Ser # # Ser # Ser # # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Ser # Seraccessed. Por ejemplo para una tienda en línea el diagrama a continuaciónilustralas posibles formas de acceder a la base de datos.

Figura2: Análisis de superficie de ataque para un sitio web de comercio electrónico

1. Los casos de uso deben abarcar:avariedad de posibles acciones que un usuario de aplicación o usuario del sistema podría realizar.

Los casos de uso deben representar la aplicación desde la perspectiva de la seguridad y pueden no abarcar todas las diferentes formas de acceder a los activos de la aplicación.

Casos de uso representan la forma en queusuariosLo ideal es que usted quiera asegurarse de que todos los requisitos de acceso que usted ha especificado en su Data ACM, sean posibles a través de uno o más Casos de Uso. Sin embargo, depende de su discreción si desea modelar los Casos de Uso basados en el acceso a roles, nivel de acceso a privilegios o acceso a datos.

1. Los componentes deben tener las pertinentes pertinencias identificadas

Los componentes son:relacionados sobre la base dela tecnología o la aplicación de la misma.es¿Qué?providesinformación muy importanteen lugar dedeterminar la susceptibilidad del componente a diversos ataques dirigidos contra las debilidades conocidas o los errores habituales cometidos durante la aplicaciónque la tecnología o el componente arquitectónico.

1. Si tiene ciertos componentes que utilizan tecnologías no disponibles para la selección en el menú desplegable mientras documenta el perfil del componente, yse puede añadir esa tecnología yendo a la tecnología caer bajo“Herramientas”->“Opciones”->”Editor de metadatos”menú. Similarly usted puede añadir autenticaciónmecanismo, tipo de servicio yclase de datosdad de identidad en un papel a modo de peso.