Para qué XP_CRYPT y SQL Shield?

Desde la Perspectiva del Gerente de Proyectos.

PARTE I: DEFINICIÓN DE LA NECESIDAD. Dónde falla la Protección de SQL Server?

Protección de Datos a Nivel de Campo

Sorprendentemente, el SQL Server no encripta los datos a nivel de campo. El acceso a los datos es concedido al registrarse en la base de datos. Pero la verdad es que si alguien tiene acceso al sistema de archivos, puede simplemente copiar los archivos de la base de datos, pegarlos en un SQL Server en el cual tenga los permisos de Administrador del Sistema, teniendo así acceso completo a sus datos.

Por lo tanto la verdad en lo que respecta a la seguridad de SQL Server es que es fuerte, mientras nadie pueda ingresar a su sistema de archivos. Con tantos exploits y hackers allí afuera, hay que tener mucha confianza cuando se es responsable de la protección de datos particularmente sensibles (como números de tarjetas de crédito, información de salud, etc).

Protección de los Procedimientos de Almacenar y de Scripts

SQL Server le permite al desarrollador codificar la lógica dentro de la base de datos. Esta lógica es guardada como procedimientos almacenados, disparadores, y funciones definidas por el usuario. Hay un par de rezones por las cuales Ud. debe querer encriptar esta lógica:

Primero, hay temas de la propiedad intelectual. Si alguien puede ver su lógica de programación, es lo mismo que vea su código fuente. Esto significa que pueden comprender los procedimiento internos “secretos” de su proyecto, y esto hace que la ingeniería inversa sea mucho más sencilla.

Segundo, si alguien puede mirar sus procedimientos almacenados, los puede editar fácilmente. Esto significa que pueden reescribir sus procedimientos almacenados y poner una lógica especial en ellos, que afectará su base de datos. Que significa esto? Las posibilidades pueden incluir desde que le borren datos, o que quiebren su base de datos, hasta actos más siniestros como robar. Por ejemplo, disponiendo de datos médicos secretos escritos o recuperados si una ficha especial es "suministrada", o quizás en una aplicación de comercio electrónico, acreditando dinero a la cuenta de una persona en lugar de debitar cada vez que compran algo.

Muchos desarrolladores argumentarían que muchos ítems "deberían" estar encriptados a nivel de campo de la base de datos. Estos ítems pueden incluir números de tarjetas de crédito, Números de Seguridad Social, y otros datos privados, como información médica.

Suena espeluznante, no? Bueno, por suerte hay una solución a ambos problemas…

PARTE II: SOLUCIÓN DE CÓDIGO – Cómo proteger con Éxito el Código SQL

Protección de Scripts…

Abra su archivo de ayuda en SQL Server, y aprenderá rápidamente que SQL Server SÍ ofrece encriptación para Procedimientos Almacenados y Scripts. Pero antes de que suspire aliviado, he aquí lo que el archivo de ayuda no le dice: en 5 minutes usted puede navegar por la web y descargar sin costo uno de los muchos programas que pueden desencriptar sus Procedimientos Almacenados "encriptados por Microsoft" en un instante. Esto significa que cualquier hacker que valga un grano de sal, tendrá la habilidad de ingresar en su código SQL y hacer lo que quiera aún si usted encriptó sus scripts utilizando el encriptado "nativo" de SQL Server.

Qué puede hacer? Bueno, felizmente el SQL Shield ofrece un encriptado de sus Procedimientos Almacenados que ningún programa de hackeado conocido puede desencriptar. Esto significa que cuando el hacker ve que sus scripts están encriptados, no importa cuántas veces intente utilizar las herramientas disponibles de hackeado, no podrá desencriptar sus códigos de scripts de SQL, lo que le da seguridad.

Al final, se está volviendo cada vez más importante proteger sus datos.

PARTE III: SOLUCIÓN DE DATOS – Cómo Aumentar la Protección de los Datos SQL

Hay muchos algoritmos diferentes que pueden usarse para encriptar sus datos. XP_CRYPT incluye RSA (algoritmo asimétrico), AES, Triple DES, DESX y RC4

(algoritmos simétricos). Usted puede elegir un algoritmo dependiendo de sus necesidades.

Sin embargo, note que los algoritmos asimétricos son de encriptación relativamente lenta comparados con los algoritmos simétricos.

La encriptación de los campos de datos es un instante con XP_CRYPT, usando la XP_CRYPT GUI, que es básicamente un programa que inyectará fácilmente rutinas de código en su base de datos.
La XP_CRYPT GUI automatiza una cantidad significativa de trabajo. Agrega todo el código de interfaz y de soporte, y lo aplica a su base de datos. Usted puede agregar fácilmente múltiples algoritmos, cada uno son sus propias claves. Debido al agregado de datos de algunos de los algoritmos más poderosos, puede ser sin duda prudente ofrecer distintos tipos de encriptado a diferentes tipos de campos, basados en el largo y tipo del campo, y la importancia de su seguridad.

En menos de 5 minutos usted puede encriptar campos en su base de datos. El programa se encargará de lo siguiente:

1) Crear tablas para administrar sus contraseñas
2) Crear campos que sean la representación encriptada de los campos que usted elija (usted borra a mano los campos con texto claro).
3) Crea una visión que desencripte los campos que usted encriptó
4) Un procedimiento de activar y llevar un registro de la clave de desencriptado para la sesión del usuario.

Las imágenes a continuación ilustran algunas de las pantallas utilizadas para agregar encriptado a nivel de campo a su base de datos.

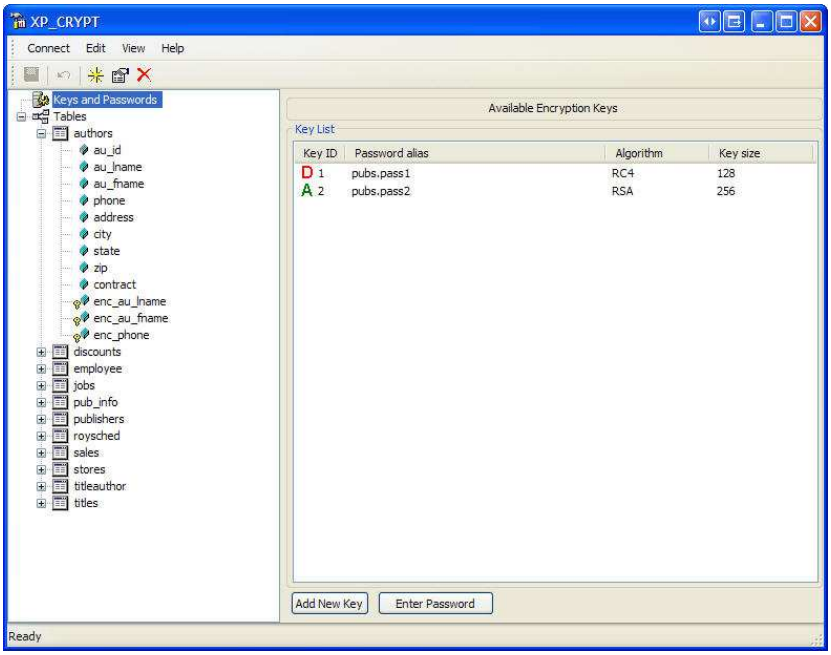

Figura 1 – Aquí se pueden agregar múltiples tipos de encriptado a la base de datos utilizando la XP_CRYPT GUI

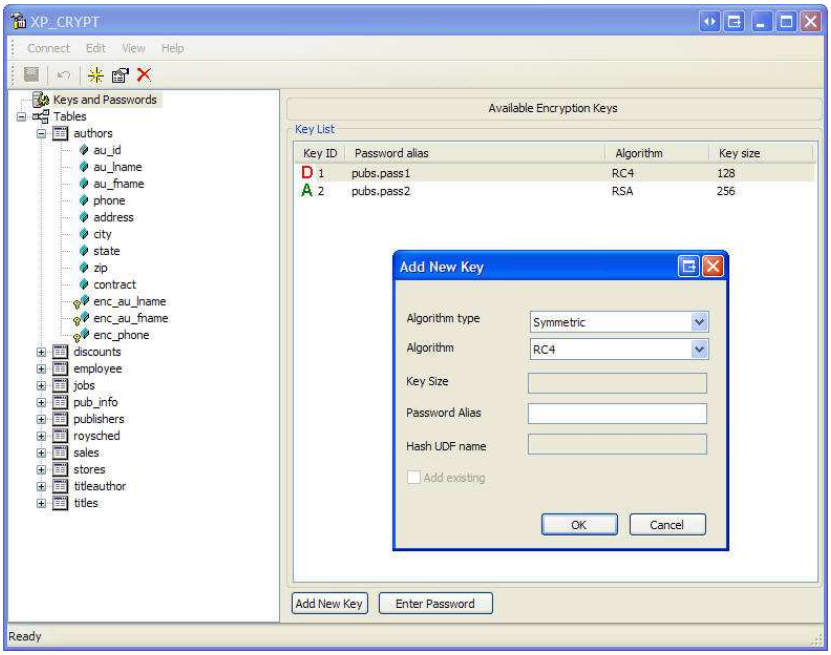

figura 2 – Aquí se pueden determinar atributos a una clave dada de encriptado. Se soportan diferentes algoritmos, incluyendo encriptado simétrico y asimétrico.

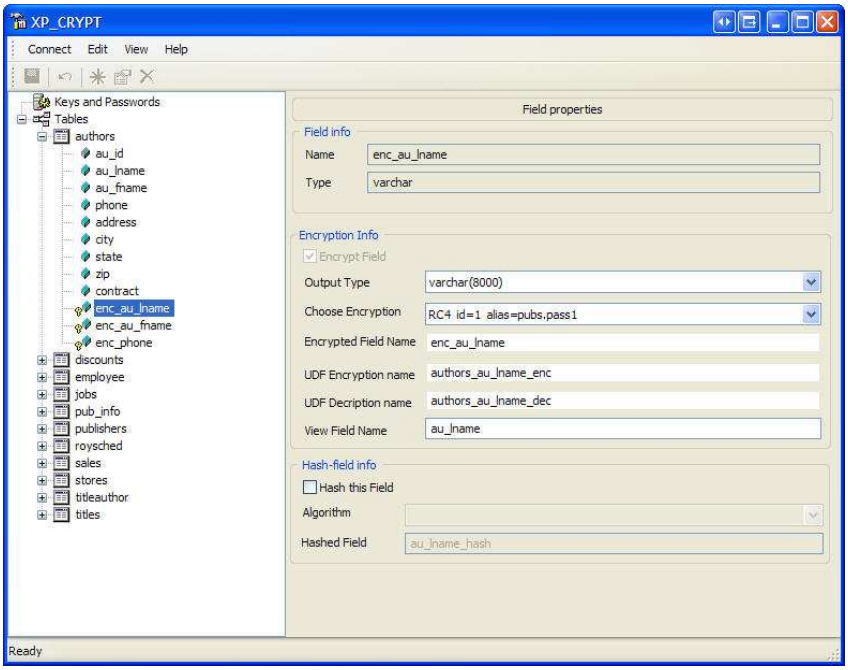

figura 3 – Aquí podemos aplicar los algoritmos de encriptado al(los) campo(s) y elegir el tipo de salida, de encriptado, y los nombres de los campos para los procedimientos que hace la XP_CRYPT GUI.

PARTE IV: ARMADO DEL CASO – Comprar Versus Construir.

A veces cuando se evalúa una herramienta, uno necesita preguntarse si es mejor comprar o construir.

1) Los Procedimientos Almacenados Extendidos **deben estar libres de errores**. Un procedimiento almacenado mal extendido llamado habitualmente por su base de datos puede colgar o corromper su base de datos. El hecho de que XP_CRYPT sea un producto comercial que ha sido utilizado por muchos usuarios reduce este riesgo.
2) Una ventaja de construir su propia solución es que usted se queda con el código fuente. Afortunadamente, usted puede comprar la **versión con código fuente** de XP_CRYPT .
3) **El tiempo es dinero**. Construir usted mismo requerirá mucho dinero, si usted desea tener soporte de múltiples algoritmos y probarlos bien. Además la buena XP_CRYPT GUI hace que sea muy fácil la rápida puesta en marcha.
4) Cuánto valen sus datos? O mejor aún, qué es lo peor que podría pasar si sus datos pierden su integridad, o usted no puede desencriptarlos? Problemas como estos pueden ocurrir si hay errores. Gastar varios miles de dólares por su tranquilidad

es mucho mejor que tener que preocuparse si el error reside en un procedimiento almacenado, o en su propio código de encriptado. Si los **datos son muy valiosos**, pregúntese sobre los costos de si las cosas no andan bien en su base de datos.

5) Es una **solución probada**. XP_CRYPT está siendo usado ya por organizaciones de gobierno de los EUA, empresas financieras, organizaciones médicas, y universidades en todo el mundo.
6) Licenciamiento - XP_CRYPT ofrece múltiples opciones de licenciamiento. El **precio es muy razonable**, ya que el precio del XP_CRYPT es una fracción del de la competencia. Las opciones de las licencias incluyen:

    a. Licencia **Única** para un servidor
    b. Puede comprarse una licencia de **Sitio** que cubrirá a todos los servidores de la empresa
    c. La licencia **Redistribuible** es para fabricantes de software que revenden la solución que quieren proteger, así que usted puede incluir su tecnología en el software que se entrega.

Cuando usted toma en consideración los pros y los contras de escribir su propia solución, usted verá muy rápidamente que una solución de un precio razonable con el código fuente es el camino correcto. Afortunadamente XP_CRYPT es una gran solución y está disponible a un buen precio*!*