Encrypting Files

أيمن حمدان الرويلي
421003512

الفهرس:

المقدمة	**1**
التشفير Encryption	**1**
تشفير الملفات Encrypting Confidential Information (EFS)	**1**
ملاحظات حول تشفير EFS	**1**
تشفير البيانات المرسلة بين المستعرض والملقم IIS باستخدام Secure Socket Layer , وتكتب اختصارا SSL	**2**
أذونات NTFS : (NTFS permissions)	**3**
أذونات IIS : (IIS permissions)	**3**
الاتصال المشفر بموقع الويب : (Enabling a Secure Encrypted Connection)	**4**
الشبكة الوهمية (الافتراضية) الخصوصية VPN (Virtual Private Network)	**5**
المراجع	**6**

المقدمة:

تتحدث هذه الورقة عن نظام تشفير الملفات **EFS .**
الموجود في ويندوز XP و لمحة موجزة عن كيفية عمله للمستخدم .

التشفير Encryption :

يستخدم ويندوز XP التشفير لعدة أهداف :
1- تشفير الملفات في وحدة تخزين NTFS , Encryption File System , وتكتب اختصارا (EFS) .
2- تشفير البيانات المرسلة بين المستعرض والملقم IIS باستخدام Socket Layer Secure , وتكتب اختصارا SSL .
3- تشفير البيانات المرسلة بين الحاسبات والشبكات (بمعظم أنواعها) باستخدام شبكة خصوصية وهمية (VBN) .

تشفير الملفات Encrypting Confidential Information (EFS) :

يزود EFS في ويندوز XP وسابقه ويندوز Server 2000 تشفيرا آمنا للمجلدات والملفات المهمة للمستخدمين , والتشفير بذاته يعتبر مستوى إضافيا من الحماية يتخطى ذلك الذي تزوده أذونات NTFS (التي تعتبر ضعيفة الأمن الى حد ما) والتي تستخدم عادة لحصر الوصول إلى الملفات الخاصة من قبل الآخرين الذين يسجلون الدخول الى نفس النظام .
ويستخدم هذا النوع من التشفير مفتاح المستخدم المعمومي لإنشاء مفتاح تشفير مولّد عشوائيا (FEK) ويقوم ويندوز تلقائيا باستعمال هذا المفتاح كلما تمت الكتابة في الناحية المشفرة سواء كانت قرصا كاملا او مجلد معين , ولا يمكن فك التشفير إلا بواسطة شهادات المستخدم والمفتاح الخصوصي الذي يتوفر فقط عند تسجيل الدخول الى النظام بواسطة اسم المستخدم وكلمة المرور الخاصة به , وهنا تجدر الإشارة الى أنه اذا تم الدخول بغير اسم المستخدم وكلمة المرور التي تم بواسطتها بناء المفتاح العمومي فلن يتم فك التشفير وستتلقى إشارة تفيد انه لا يمكنك الوصول الى هذا المجلد او الملف .

ملاحظات حول تشفير EFS :

1- عندما تستعمل التشفير للمرة الأولى يقوم ويندوز تلقائيا بإنشاء شهادة خاصة بهويتك لـــ EFS وهي بمثابة شهادة تشفير شخصية وتحتوي على مفتاحين الأول عمومي والثاني خصوصي لإستعمالهما في تشفير وفك التشفير بينما تكون مسجلا دخولك الى النظام .
ويمكن إنشاء شهادة تشفير شخصية باستخدام اداة التشفير Cipher.exe من موجه الاوامر ..
ولتشفيرمجلد My Documents اتبع أكتب السطر التالي :
Cipher.exe/e/a/s:"%userprofile%my documents
ويمكنك تشفير أكثر من مجلد بدكر اسم المجلدات سوية ووضع فراغ بين هذه الأسماء .
كما يمكنك فعل ذلك من خلال الضغط باليمين على المجلد واختيار Properties ثم General ثم Advanced ثم اختيار Encrypt contents to secure data ...
واذا شفرت مجلدا معينا فيكفي لتشفير ملف ما أن تنقل هذا الملف الى داخل المجلد وهنا سيتم تشفيره بشكل تلقائي.
2- تشفير EFS يعد تشفيرا آمنا لدرجة أنك إذا فقدت المفتاح لفك تشفير البيانات ستكون قد فقدت البيانات المشفرة بالكامل ولايوجد (إلى الآن) بابا خلفيا للحيلولة دون ذلك .

3- لا يمكن تشفير أي ملف من ملفات النظام وهي التي تكون عادة سمتها System وإذا نقلت الملف المشفر إلى وحدة تخزين FAT فهنا سيتم فك تشفيره اذا كنت مسجلا بمفتاحك الخاص , وأما إذا نقله غيرك إلى وحدة تخزين FAT وحاول فتحه فستظهر رسالة (الوصول ممنوع) .
وأما إذا نقلت الملف المشفر إلى وحدة تخزين مشابهة أي (NTFS) فسيبقى محافظا على تشفيره .
4- هناك الكثير من الخصائص التي يمكنك استخدامها مع EFS كإنشاء وكيل استعادة بيانات وعكل نسخة احتياطية لمفتاحك الخاص وتحديد المسموح لهم بمعاينة ملفاتك المشفرة وغيرها من الخصائص التي تجعل من هذا النوع من التشفير نظاما متكاملا وبموثوقية عالية .

تشفير البيانات المرسلة بين المستعرض والملقم IIS باستخدام Secure Socket Layer , وتكتب اختصارا SSL :

أمن الاتصال باستخدام IIS :
يزود IIS وويندوز XP سوية ثلاث يتم من خلالها التحكم بالوصول الى الدلائل والملفات في موقع الوب وهي :
1- التحقق من الصحة . (Authentication)
2- أذونات (NTFS permissions) . NTFS)
3- أذونات (IIS permissions) . IIS)

ولنبدأ بتفصيل هذه الانواع :
التحقق من الصحة . (Authenication)
هي عملية يحدد بها ويندوز وIIS من يحاول الوصول الى ملف معين في موقع الويب , وما اذا كان هذا الشخص مصرح له بذلك أم لا .
ويتيح IIS ثلاثة اشكال للتحقق من الصحة :
1- التحقق من الصحة الأساسي : Basic Authentication :
هذا النوع هو أقل الأنواع الثلاثة أمنا لأنه يرسل معلومات المستخدم من اسم الحساب وكلمة المرور باستخدام التشفير Base64 وهذا النوع من التشفير يوجد الكثير من الادوات التي يتم من خلالها اعتراض طريقه وأدوات مخصصه لفكه , إلا أن ميزاته تكمن في أنه جزء من المواصفات القياسية HTTP 1 أي أنه يمكن أن يستخدم أي مستعرض ويب وفي أي نظام تشغيل , وكونه لا يتميز بتقنيات تشفير معقدة وقوية فهذا يجعل الاتصال من خلاله أسرع من غيره , ويمكننا جعله اكثر أمنا باستخدام SSL معه وسيأتي تفصيل ذلك لاحقا .
يتيح هذا النوع للعميل تكرار محاولة تسجيل الدخول الى النظام ثلاث مرات قبل أن يعطيه رسالة الوصول ممنوع (Access Denied).
2- التحقق من الصحة المتقدم : (authentication Advanced digest)
يستخدم هذا النوع من التحقق طريقة أكثر أمنا من سابقه , ويتم من خلاله ارسال الطلبات او تسجيل الدخول باستخدام تشفير البعثرة (Hash Coding) بتقنية MD5 (خوارزميات البصمة الإلكترونية وهذه الخوارزميات هي اقترانات تمويه يُمكن تطبيقها على التواقيع الرقمية بدأ ظهورها عام 1989 بواسطة Ronald Rivest), حيث يرسل IIS اسم النطاق او المجال الى مستعرض المستخدم ويطلب منه تسجيل الدخول ثم ينشئ بعثرة MD5 من اسم النطاق ومن معلومات المستخدم ويرسل هذه البعثرة إلى IIS الذي بدوره يسلمها الى متحقق النطاق أو الميدان ليتم التحقق منها .
وهذا النوع موجود طبعا في نسخة ويندوز Server 2000 إلا أنه في ويندوز XP صار أكثر أمنا من سابقه حيث أنه يتم في ويندوز Server 2000 تخزين كلمة مرور المستخدم من خلال نص عادي على الملقم , أما في ويندوز XP فيتم تخزينها كبعثرة MD5 كما تقدم ..
ولابد لهذا النوع أن يكون المستخدم لديه انترنت اكسبلورر النسخة 5 أو ما يليه .

3- التحقق من الصحة المندمج او المتكامل مع ويندوز : (Integrated Windows authentication)
هذا النوع هو أكثر الانواع الثلاثة أمنا وذلك لأنه لا يطلب من المستخدم تسجيل دخوله عبر الشبكة وإنما يتأكد من الصحة من خلال تبادل ترميز بين المستخدم و IIS باستخدام عنونة عشوائية (Hashing) أحادية الاتجاه , ومشكلة هذا النوع من التحقق أنه لا يعمل على اتصالات HTTP الوكيلة , ويستلزم هذا النوع من التحقق أن يكون المستخدم او العميل يشغل انترنت اكسبلورر اصدار او ما يليه .
وهذا النوع من التحقق لا يتيح للمستخدم أي فرصة لمجرد الخطأ في إدخل بياناته لذا فإنه يعطي رسالة الوصول ممنوع (Access Denied) بمجرد الخطأ في المرة الاولى من إدخال البيانات .
وقبل أن أختم الحديث عن التحقق من الصحة أضيف أنه هناك خيار رابع وهو الوصول المجهول (Anonymous Authentication) واستعمال هذا النوع يعني ان الموقع متوفر لأي عميل لأنه لن يُطلب من المستخدم ادخال بيانات التسجيل ..
ويتم استخدام هذا النوع من الاتصال من خلال حساب خاص يسمى IUSR_computername وهذا الحساب لا يستطيع المستخدم أن يير كلمة المرور فيه وأيضا لا تنتهي صلاحية كلمة المرور أبدا .
ولكن لا يفضل استخدام هذا النوع من الوصول الا في الظروف التي تكون فيها الحاجة الى الأمن منخفضة جدا خاصة انك بهذا الخيار تجعل جميع موارد موقعك متوفرة للجميع .

أذونات NTFS : (NTFS permissions)

هذه الميزة خاصة بالنظام وليست للملقم IIS ويمكنك من خلالها وضع قواعد مختلفة لحسابات المستخدمين أو حتى مجموعة حسابات مختلفة تحدد لكل مستخدم أو مجموعة خيارات خاصة بها للوصول إلى الملفات , كأن تجعل لأحدهم خيار تحكم كامل بالملف ولآخر القراءة فقط .. وهكذا .... ويمكن تطبيقها على الملفات والمجلدات في أي محرك أقراص مهيأ بـــ NTFS .
ولعل الفائدة من هذه الأذونات تتجلى أكثر من خلال دمجها مع ميزة (Sharing) التي أقلقت مايكروسوفت بثغرتها المشهورة , وبالتالي تم تطويرها في XP وأصبحت تدعى (Simple File Sharing) مقابل أسلوب المشاركة المعروف سابقا في إصدارات ويندوز , فعندما تريد عمل مشاركة لملف ما أو محرك أقراص بواسطة ويندوز XP يتعين عليك أن تضبط أذونات المشاركة ذاتها وأذونات ملفات NTFS مما يجعلها أكثر أمنا من السابق , وهذا طبعا سواء بالنسبة للمشاركة مع المستخدمين المحليين أو مستخدمي الشبكة .
لرؤية ما هو تأثير كل أذونات NTFS على مستخدم أو مجموعة مستخدمين نفذ الخطوات التالية :

افتح مربع حوار خصائص ملف أو مجلد ثم اختر Properties ثم انقر علامة التبويب Security من خلالها يمكنك معرفة خصائص أي مستخدم أو مجموعة ما يمكنها الوصول إليه أو لا
كما تلاحظ يظهر لكل مستخدم الخيارات الخاصة به ... ويمكنك الذهاب إلى الأذونات الخاصة بالنقر على Advanced

أذونات IIS : (IIS permissions)

تتحكم أذونات IIS بما يستطيع أن يفعله المستخدمون بعد وصولهم إلى مورد في موقع الويب , ويتم تطبيقها بشكل متساوي على جميع المستخدمين , كما يمكن تطبيقها على الملفات أو الدلائل أو حتى على موقع بأكمله .
ولها عدة خيارات منها :
Read : تتيح للمستخدمين قراءة محتوى وخصائص ملف ما أو صفحة أو دليل معين .
Write : تتيح للمستخدمين تغيير محتوى أو خصائص ملف ما أو دليل معين .
Script Source Access (الوصول إلى مصدر النص البرمجي) : وتتيح للمستخدمين الوصول إلى الملفات المصدر , وإذا كان الخيار (Read) منتقى أيضا فسيتمكن المستخدمون من قراءة شفرة النص البرمجي

المصدر , وإذا كان Write)) منتقى أيضا فسيتمكنون من تعديل الشفرة , وفي حال أن Read و Write غير منتقيين فليس من الممكن الوصول إلى مصدر النص البرمجي .
Directory Browsing (استعراض الدليل): يتيح للمستخدمين معاينة دلائل الملفات .

الاتصال المشفر بموقع الويب : (a Secure Encrypted Connection Enabling)

يستطيع IIS أن يستخدم Secure Sockets Layer SSL) طبقة المقابس الآمنة ... لإنشاء اتصال مشفر بين موقع الويب وبين المستخدمين , وتستخدم SSL تشفيرا بالمفتاح العمومي إما بقوة 40 بت أو 128 بت , وعندما يسجل المستخدمين دخولهم إلى الموقع عبر اتصال آمن سيبنون عنوان URL باستخدام HTTPS بدلا من HTTP ولعلك ستلاحظ وجود (Padlock Icon) على شريط متصفحك بالأسفل تشير إلى أن الاتصال مشفر بـــ SSL ...
وهذا النوع من الاتصال يستلزم استعمل ما يسمى بـــ Digital Certificates (شهادات رقمية تتيح للملقمات والمستخدمين التحقق من صحة بعضهم البعض) ومهمة هذه الشهادات في الدرجة الأولى هي إعطاء الموثوقية للمستخدم أن السيرفر الذي يتعامل معه الآن هو نفس السيرفر المقصود وذلك حتى يمنع أي تسلل من الهكر ينتج عنه السطو على بيانات المستخدمين, وهذه العملية تتم من خلال حفظ وتخزين قاعدة بيانات الـــ DNS داخل أو ضمن الشهادات الرقمية ليتم التحقق من أن السيرفر المطلوب هو فعلا السيرفر الحقيقي , وتأتي هذه الشهادات في ثلاثة أنواع :

1- شهادة الملقم : (Server certificates) وتستعمل لتعريف الملقمات لمستعرضي الويب , ولتزويد المفتاح العمومي لتشفير SSL كلما اتصل مستخدم بمورد ما في ملقمك باستخدام البروتوكول HTTPS (على عكس HTTP) يعرّف الملقم نفسه أولا بواسطة شهادة الملقم الخاصة به , وبعد أن يقبل المستعرض الشهادة ينشأ اتصال SSL مشفر باستخدام المفتاح الخصوصي الخاص بالملقم لدى الملقم والمفتاح العمومي لدى المستعرض .
2- شهادات المستخدمين : (Client certificates) وتستعمل لتعريف مستعرضي الويب للملقمات , ويستطيع الموقع الآمن أن يجبر المستعرضين على تعريف أنفسهم بشهادة عميل كجزء من عملية التحقق من الصحة .
3- شهادة Certification Authority) : CA) سلطة الشهادات .. , تعطي قيمة الموثوقية لشهادات الملقم والعملاء حيث يحتفظ انترنت اكسبلورر بلائحة بالسلطات CA المعروفة والموثوق بها , وعندما يصل المستخدم إلى صفحة ويب آمنة يتم إرسال شهادة الملقم الخاصة بملقم الويب إلى المستعرض وهنا يفحص المستعرض السلطة CA التي أصدرت شهادة الملقم , فإذا كانت السلطة CA موجودة في لائحة السلطات CA الموثوق بها يتم قبول الشهادة تلقائيا , وإذا لم تكن السلطة CA موجودة في اللائحة يظهر مربع حوار يعطي المستخدم الخيار بقبول أو رفض الشهادة ..
ويمكن الحصول على شهادة ملقم من خلال إنشاء طلب شهادة وتسليمه إلى سلطة الشهادة والحصول عليها مصدقة ومن ثم تثبيتها في النظام , وعادة يتولى معالج شهادة ملقم الويب (Server Certificate) معظم هذه العملية .

وقبل أن أختم الكلام حول SSL أذكر أنه يمكن استعمال SSL لحماية (التحقق من الصحة الأساسي) حيث يمكن إعداد موقع الويب ليستخدم التحقق من الصحة الأساسي مع اتصال SSL , وبذلك فإنه ينشأ ارتباط SSL قبل التحقق من الصحة , لذا يتم إرسال اسم المستخدم وكلمة المرور بشكل مشفر , ولكن كل تفاعلات المستخدم مع الموقع ستستعمل SSL وبالتالي سيكون الاتصال بطيئا , ويمكن التحايل على هذا بطريقة (غير عملية) وهي من خلال تثبيت شهادة الملقم في موقع الويب وجعل استخدام SSL اختياريا للمستخدم , فإذا أراد إرسال معلومات مهمة فما عليه إلا تبديل العنوان URL من HTTP إلى HTTPS ويمكنه إكمال تصفح ما يرى تشفيره غير ضروري باستخدام HTTP ..... وبالتالي لن يكون هناك أي بطئ إلا عند استخدام SSL ....

يمكنك تركيب سيرفر IIS بنفسك وتجربة ما تعلمته الآن فقط اذهب إلى Panel Control ثم Administrative Tools ثم Internet Information Services ....

الشبكة الوهمية (الافتراضية) الخصوصية VPN (Virtual Private Network)

هي عبارة عن وسيلة اتصال بشبكة خصوصية (كشبكة شركة ما) من خلال شبكة عمومية كالانترنت ويمكن من خلالها استخدام كل موارد وبروتوكولات الشبكة الخصوصية تماما ...
ويتم ذلك من خلال طريقة آمنة وفعالة لوصل الشبكتين باستخدام بروتوكولات Tunneling (النفق أو القناة) التي ترسل البيانات تحت بروتوكول الشبكة الوسيطة (الانترنت) لكي توحي أن هناك مسارا مباشرا بين الشبكتين المفصولتين .
وإرسال البيانات خلال بروتوكولات (النفق) يتم بطريقة مشفرة (بتقنية EFS) تعتمد على تشفير كل رزمة IP وتغليفها داخل رزمة أخرى مع إعطائها عنونة جديدة لترسل عبر الشبكة الوسيطة , وعندما تصل الرزم المشفرة والمعنونة من جديد إلى الجهة الأخرى يتم إعادة عنونتها وفك تشفيرها كما كانت في الشبكة الأصلية .... وهكذا تحصل على شبكة خصوصية وهمية .

هناك ثلاثة أنواع من بروتوكولات الأنفاق وهي :

1- PPTP ... Point-to-Point Tunneling Protocol ... ويتيح تشفير رزم IP أو IPX أو NetBeui ثم تغليفها ليتم إرسالها عبر الشبكة الوسيطة .
2- L2TP ...Protocol Layer 2 Tunneling ويتيح تشفير رزم IP أو IPX أو NetBeui ثم تغليفها ليتم إرسالها عبر شبكة وسيطة أو X.25 أو Frame Relay أو ATM ..
3- IP ... Security Tunnel Mode IPSec .. ويتيح أيضا تشفير رزم IP ثم تغليفها وإرسالها .
أشير هنا إلى أن ويندوز 2000 يستخدم لمثل هذه الاتصالات بروتوكول L2TP بينما يستخدم ويندوز XP PPTP أو L2TP كما يستخدم ويندوز XP أيضا IPSec لتحسين أمان كل تفاعلات الشبكة .

المراجع:

http://www.microsoft.com/TechNet/security/topics/analefs.asp
http://microsoft.com/windows2000/techinfo/howitworks/security/encrypt.asp
http://support.microsoft.com/support/kb/articles/q143/4/75.asp
John[1].Wiley.and.Sons.Network.Security.Bible.Jan.2005.eBook-DDU
http://www.researchindex.org/