इंटरनेट एक्सप्लोरर पासवर्ड रिकवर करना: सिद्धांत और व्यवहार

पास्केप सोफ्टवेर (हिन्दी अनुवाद : धीरेन कुमार)

परिचय

1 परिचय

कोई भी इस तथ्य पर विवाद नहीं करेगा कि **इंटरनेट एक्सप्लोरर** आज का सबसे लोकप्रिय वेब ब्राउज़र है। आंकड़ों के अनुसार, लगभग 70% ऑनलाइन यूजर केवल इस कार्यक्रम का उपयोग करना पसंद करते हैं। इसके पेशेवरों और विपक्षों के बारे में तर्क हमेशा के लिए चल सकते हैं; फिर भी, यह ब्राउज़र अपने उद्योग में सबसे आगे है, और यह एक ऐसा तथ्य है जिसके लिए किसी प्रमाण की आवश्यकता नहीं है। इंटरनेट एक्सप्लोरर में कई अंतर्निहित तकनीके हैं, जो औसत यूजर के जीवन को आसान बनाने के लिए डिज़ाइन की गई हैं। उनमें से एक - **IntelliSense** - नियमित कार्यों का ध्यान रखने के लिए बनाया गया है, जैसे विज़िट किए गए वेबपेज पतों को स्वचालित रूप से पूरा करना, फ़ॉर्म फ़ील्ड को स्वचालित रूप से भरना, यूजर्स के पासवर्ड आदि।

आज की कई वेबसाइटों में पंजीकरण की आवश्यकता होती है, जिसका अर्थ है कि यूजर को यूजर नाम और पासवर्ड दर्ज करना होगा। यदि आप एक दर्जन से अधिक ऐसी वेबसाइटों का उपयोग करते हैं, तो आपको एक पासवर्ड मैनेजर की आवश्यकता होगी। सभी आधुनिक ब्राउज़रों में उनके शस्त्रागार में एक अंतर्निहित पासवर्ड मेनेजर होता है, और इंटरनेट एक्सप्लोरर एक अजीब नहीं है। वास्तव में, किसी को एक और पासवर्ड क्यों याद रखना होगा यदि वह किसी भी समय जल्द ही भूल जाने वाला है? आपके लिए पासवर्ड याद रखने और संग्रहीत करने का नियमित कार्य ब्राउज़र द्वारा करना बहुत आसान होगा। यह सुविधाजनक और आरामदायक है।

यह बिल्कुल सही समाधान होगा; हालांकि, यदि आपका विंडोज ऑपरेटिंग सिस्टम क्रैश या रीइंस्टॉल हुआ है, तो आप आसानी से अपने कीमती पासवर्ड की पूरी सूची खो सकते हैं। आराम और सुविधा के लिए यह कर है। यह अच्छा है कि प्रत्येक वेबसाइट में 'मैं पासवर्ड भूल गया' बटन सहेज रहा हूं। हालांकि, यह बटन हमेशा आपका सिरदर्द आपसे दूर नहीं करेगा।

प्रत्येक सॉफ़्टवेयर डेवलपर भूल गए पासवर्ड रिकवरी समस्या को अपने तरीके से हल करता है। उनमें से कुछ आधिकारिक तौर पर कुछ महत्वपूर्ण फाइलों को दूसरे फ़ोल्डर में कॉपी करने की सलाह देते हैं, जबकि अन्य सभी पंजीकृत यूजर्स को एक विशेष यूटिलिटी भेजते हैं जो निजी डेटा के प्रवासन को प्रबंधित करने की अनुमति देता है, और तीसरे लोग दिखावा करते हैं कि वे समस्या नहीं देख रहे हैं। फिर भी, मांग प्रस्ताव बनाती है, और पासवर्ड रिकवरी कार्यक्रम वर्तमान में बहुत मांग में हैं।

इस लेख में, आइए इंटरनेट एक्सप्लोरर में संग्रहीत निजी डेटा के प्रकारों को वर्गीकृत करने का प्रयास करें, डेटा की रिकवरी के लिए कार्यक्रमों को देखें, और खोए हुए इंटरनेट पासवर्ड को रिकवर करने के वास्तविक जीवन के उदाहरणों का अध्ययन करें।

इंटरनेट एक्सप्लोरर में संग्रहीत पासवर्ड के प्रकार

2 इंटरनेट एक्सप्लोरर में संग्रहीत पासवर्ड के प्रकार

इंटरनेट एक्सप्लोरर निम्नलिखित प्रकार के पासवर्ड स्टोर कर सकता है:

- इंटरनेट क्रेडेंशियल
- स्वत: पूर्ण डेटा
- स्वतः पूर्ण पासवर्ड
- FTP क्रेडेंशियल
- कैश्ड वेबसाइटों के लिए सिंक्रोनाइज़ेशन पासवर्ड
- पहचान पासवर्ड
- ऑटोफॉर्म डेटा
- कन्टेन्ट एडवाइजर पासवर्ड

आइए प्रत्येक सूचीबद्ध आइटम पर करीब से नज़र डालें।

2.1 इंटरनेट क्रेडेंशियल

इंटरनेट क्रेडेंशियल्स का अर्थ है यूजर के लॉगिन और पासवर्ड जो कुछ वेबसाइटों तक पहुँचने के लिए आवश्यक हैं, जिन्हें wininet.dll लाइब्रेरी द्वारा संसाधित किया जाता है। उदाहरण के लिए, जब आप किसी वेबसाइट के संरक्षित क्षेत्र में प्रवेश करने का प्रयास करते हैं, तो आप निम्न यूजर नाम और पासवर्ड संकेत (चित्र 1) देख सकते हैं।

चित्र 1. इंटरनेट क्रेडेंशियल संवाद।

यदि उस प्रांप्ट में 'मेरा पासवर्ड याद रखें' विकल्प चुना जाता है, तो यूजर क्रेडेंशियल आपके स्थानीय कंप्यूटर में सहेजे जाएंगे। Windows 9x के पुराने वर्जनो ने उस डेटा को यूजर की **PWL फ़ाइल** में संग्रहीत किया; Windows 2000 और नए इसे **प्रोटेक्टेड स्टोरेज** में स्टोर करते हैं।

USERNAME.PWL (जहाँ USERNAME आपका लॉगऑन नाम है) एक पासवर्ड सूची फ़ाइल है। यह नेटवर्क पर संसाधनों के लिए पासवर्ड रिकॉर्ड करता है और उन संसाधनों से पुन: कनेक्ट करने के लिए उनका उपयोग करता है ताकि आपको फिर से पासवर्ड टाइप न करना पड़े।

प्रोटेक्टेड स्टोरेज यूजर डेटा को संग्रहीत करने के लिए एक इंटरफ़ेस के साथ एप्लिकेशन प्रदान करता है जिसे सुरक्षित या संशोधन से मुक्त रखा जाना चाहिए। संग्रहीत डेटा की इकाइयों को आइटम कहा जाता है। संग्रहीत डेटा की संरचना और सामग्री संरक्षित संग्रहण प्रणाली के लिए अपारदर्शी है। आइटम तक पहुंच यूजर द्वारा परिभाषित सुरक्षा शैली के अनुसार पुष्टि के अधीन है, जो निर्दिष्ट करती है कि डेटा तक पहुंचने के लिए किस पुष्टिकरण की आवश्यकता है, जैसे कि पासवर्ड की आवश्यकता है या नहीं। इसके अलावा, आइटम तक पहुंच एक एक्सेस नियम सेट के अधीन है। प्रत्येक एक्सेस मोड के लिए एक एक्सेस नियम है: उदाहरण के लिए, पढ़ना/लिखना। एक्सेस नियम सेट एक्सेस क्लॉज से बने होते हैं। आमतौर पर एप्लिकेशन सेटअप समय पर, एक नए एप्लिकेशन को यूजर से आइटम तक पहुंच का अनुरोध करने की अनुमति देने के लिए एक तंत्र प्रदान किया जाता है जो पहले किसी अन्य एप्लिकेशन द्वारा बनाया गया हो सकता है।
की, प्रकार, उपप्रकार और नाम के संयोजन से आइटम विशिष्ट रूप से पहचाने जाते हैं। की एक कोन्स्टंट है जो निर्दिष्ट करता है कि आइटम इस कंप्यूटर के लिए वैश्विक है या केवल इस यूजर के साथ संबद्ध है। नाम एक स्ट्रिंग है, जिसे आम तौर पर यूजर द्वारा चुना जाता है। प्रकार और उपप्रकार GUID हैं, जो आमतौर पर एप्लिकेशन द्वारा निर्दिष्ट किए जाते हैं। प्रकार और उपप्रकारों के बारे में अतिरिक्त जानकारी सिस्टम रजिस्ट्री में रखी जाती है और इसमें प्रदर्शन नाम और UI संकेत जैसी विशेषताएँ शामिल होती हैं। उपप्रकारों के लिए, मूल प्रकार निश्चित है और सिस्टम रजिस्ट्री में एक विशेषता के रूप में शामिल है। प्रकार समूह आइटम का उपयोग एक सामान्य उद्देश्य के लिए किया जाता है: उदाहरण के लिए, भुगतान या पहचान। उपप्रकार समूह आइटम एक सामान्य डेटा प्रारूप साझा करते हैं।
हम आगामी लेखों में से किसी एक में संरक्षित संग्रहण संरचना को कवर करने का प्रयास करेंगे।

2.2 ऑटो-कम्प्लेट डेटा

ऑटो-कम्प्लेट डेटा (पासवर्ड आगे कवर किया जाएगा) भी संरक्षित संग्रहण में संग्रहीत किया जाता है और HTML प्रपत्र फ़ील्ड नामों और संबंधित यूजर डेटा की सूची के रूप में प्रकट होता है। उदाहरण के लिए, यदि किसी HTML पृष्ठ में एक ई-मेल पता प्रविष्टि संवाद है: एक बार जब यूजर अपना ई-मेल पता दर्ज कर लेता है, तो संरक्षित संग्रहण में HTML फ़ील्ड का नाम, पता मान और रिकॉर्ड तक पहुंचने का समय होगा।

HTML पृष्ठ का शीर्षक और वेबसाइट का पता संग्रहीत नहीं है। वह अच्छा है या बुरा है? यह निर्धारित करना मुश्किल है; बुरे से अच्छा होने की अधिक संभावना है। यहाँ स्पष्ट लाभ हैं: यह खाली स्थान बचाता है और ब्राउज़र के प्रदर्शन को गति देता है। यदि आपको लगता है कि अंतिम नोट महत्वहीन है, तो यह कल्पना करने का प्रयास करें कि आपको एक बहु-हजार में कई अतिरिक्त चेकअप कैसे करने होंगे (यह उतना दुर्लभ नहीं है जितना यह प्रतीत हो सकता है) ऑटो-फिल सूची।

एक और स्पष्ट प्लस यह है कि समान नाम के लिए डेटा (और अक्सर विषय के अनुसार) HTML फॉर्म फ़ील्ड को उसी स्थान पर संग्रहीत किया जाएगा, और सामान्य डेटा का उपयोग ऐसे पृष्ठों को स्वचालित रूप से भरने के लिए किया जाएगा। इसे हम इस उदाहरण से देखेंगे। यदि एक HTML पृष्ठ में 'ईमेल' नाम के साथ एक स्वतः-भरण फ़ील्ड है, और यूजर ने उस फ़ील्ड में अपना ई-मेल पता दर्ज किया है, तो IE संग्रहण में, मोटे तौर पर, 'email=my@email.com' डाल देगा। अब से, यदि यूजर कोई अन्य वेबसाइट खोलता है, जिसमें समान फ़ील्ड नाम 'ईमेल' वाला एक पृष्ठ है, तो उपयोगकर्ता को सुझाव दिया जाएगा कि वह पहले पृष्ठ पर दर्ज किए गए मान के साथ इसे स्वतः भरें (my@email.com)) इस प्रकार, ब्राउज़र कुछ हद तक अपने भीतर AI क्षमताओं का पता लगाता है।

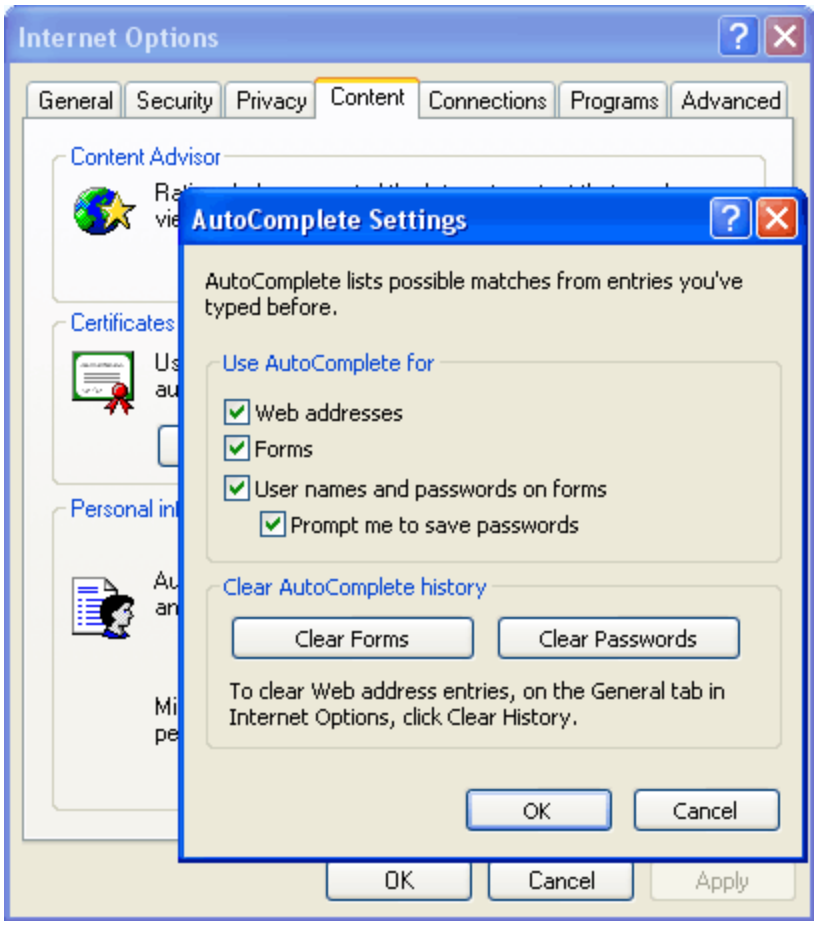
इस डेटा भंडारण पद्धति का मुख्य दोष इसके लाभ से आता है जिसका हमने अभी वर्णन किया है। कल्पना कीजिए, यूजर ने वेबपेज पर ऑटो-फिल डेटा दर्ज किया है। यदि कोई व्यक्ति HTML प्रपत्र फ़ील्ड नाम जानता है, तो वह व्यक्ति उसी फ़ील्ड नाम के साथ अपना स्वयं का सरलतम HTML पृष्ठ बना सकता है और उसे स्थानीय डिस्क से खोल सकता है। इस क्षेत्र में दर्ज किए गए डेटा को उजागर करने के लिए, ऐसे व्यक्ति को इंटरनेट से कनेक्ट करने और मूल WWW पता खोलने की भी आवश्यकता नहीं होगी।

2.3 स्वतः पूर्ण पासवर्ड

पासवर्ड डेटा के मामले में, हालांकि, जैसा कि आपने अनुमान लगाया होगा, डेटा स्वचालित रूप से नहीं भरा जाएगा। चूंकि ऑटो-पूर्ण पासवर्ड वेब पेज नाम के साथ संग्रहीत किए जाते हैं, और प्रत्येक पासवर्ड केवल एक विशिष्ट HTML पृष्ठ के लिए बाध्य होता है।

नए वर्जन में, **इंटरनेट एक्सप्लोरर 7**, स्वत: पूर्ण पासवर्ड और डेटा दोनों पूरी तरह से अलग एन्क्रिप्टेड हैं; नई एन्क्रिप्शन विधि अभी वर्णित कमी से मुक्त है (यदि इसे एक कमी के रूप में वर्गीकृत किया जा सकता है।)

यह ध्यान देने योग्य है कि इंटरनेट एक्सप्लोरर यूजर्स को विकल्प मेनू के माध्यम से मैन्युअल रूप से स्वत: भरण मापदंडों को प्रबंधित करने की अनुमति देता है, (चित्र 2)।



चित्र 2. इंटरनेट एक्सप्लोरर स्वतः पूर्ण सेटिंग्स।

2.4 FTP क्रेडेंशियल

FTP साइट क्रेडेंशियल काफी हद तक उसी तरह संग्रहीत किए जाते हैं। यह ध्यान रखना प्रासंगिक होगा कि Windows XP से शुरू होने वाले FTP पासवर्ड अतिरिक्त रूप से DPAPI के साथ एन्क्रिप्ट किए जाते हैं। यह एन्क्रिप्शन विधि लॉगऑन पासवर्ड का उपयोग करती है। स्वाभाविक रूप से, इससे ऐसे खोए हुए पासवर्ड को मैन्युअल रूप से पुनर्प्राप्त करना अधिक कठिन हो जाता है, क्योंकि अब किसी को यूजर की मास्टर की, SID और अकाउन्ट पासवर्ड की आवश्यकता होगी।

2.5 सिंक्रोनाइज़ेशन पासवर्ड

सिंक्रोनाइज़ेशन पासवर्ड यूजर को कैश्ड वेबसाइटों के लिए पासवर्ड दर्ज करने से मुक्त करता है (साइटें ऑफ़लाइन उपलब्ध होने के लिए सेट हैं।) इस प्रकार के पासवर्ड भी IE के संरक्षित संग्रहण में संग्रहीत किए जाते हैं।

2.6 पहचान पासवर्ड

इसे ही पहचान पासवर्ड हैं। संभवतः **आउटलुक एक्सप्रेस** को छोड़कर, माइक्रोसॉफ्ट के उत्पादों में पहचान-आधारित पहुंच प्रबंधन तंत्र व्यापक नहीं है।

2.7 ऑटोफॉर्म डेटा

एक विशेष पैराग्राफ में फॉर्म ऑटो-फिल मेथड को कवर करना चाहिए, जो डेटा स्टोर करने का एक हाइब्रिड तरीका है। यह विधि वास्तविक डेटा को संरक्षित संग्रहण में संग्रहीत करती है, और URL, जिससे डेटा संबंधित है, यूजर की रजिस्ट्री में संग्रहीत किया जाता है। रजिस्ट्री में लिखा गया URL प्लेनटेक्स्ट के रूप में संग्रहीत नहीं है - इसे हैश के रूप में संग्रहीत किया जाता है। इंटरनेट एक्सप्लोरर 4 - 6 में फॉर्म ऑटो-फिल डेटा पढ़ने के लिए एल्गोरिदम यहां दिया गया है:

```
//Get autoform password by given URL
BOOL CAutoformDecrypter::LoadPasswords(LPCTSTR cszUrl, CStringArray
*saPasswords)
{
   assert(cszUrl && saPasswords);

   saPasswords->RemoveAll();

   //Check if autoform passwords are present in registry
   if ( EntryPresent(cszUrl) )
   {
      //Read PStore autoform passwords
      return PStoreReadAutoformPasswords(cszUrl,saPasswords);
   }

   return FALSE;
}
```

```
//Check if autoform passwords are present
BOOL CAutoformDecrypter::EntryPresent(LPCTSTR cszUrl)
{
   assert(cszUrl);

   DWORD dwRet, dwValue, dwSize=sizeof(dwValue);
   LPCTSTR cszHash=GetHash(cszUrl);

   //problems computing the hash
   if ( !cszHash )
      return FALSE;

   //Check the registry
   dwRet=SHGetValue(HKCU,_T("Software\Microsoft\Internet
Explorer\IntelliForms\SPW"), cszHash, NULL, &dwValue, &dwSize);
   delete((LPTSTR)cszHash);

   if ( dwRet==ERROR_SUCCESS )
      return TRUE;

   m_dwLastError=E_NOTFOUND;
   return FALSE;
}


//retrieve hash by given URL text and translate it into hex format
LPCTSTR CAutoformDecrypter::GetHash(LPCTSTR cszUrl)
{
   assert(cszUrl);

   BYTE buf[0x10];
   LPTSTR pRet=NULL;
   int i;

   if ( HashData(cszUrl,buf,sizeof(buf)) )
   {
      //Allocate some space
      pRet=new TCHAR [sizeof(buf) * sizeof(TCHAR) + sizeof(TCHAR)];
      if ( pRet)
      {
         for ( i=0; i<sizeof(buf); i++ )
         {
            // Translate it into human readable format
            pRet[i]=(TCHAR) ((buf[i] & 0x3F) + 0x20);
         }
         pRet[i]=_T('');
      }
      else
```

```
        m_dwLastError=E_OUTOFMEMORY;
    }

    return pRet;
}


//DoHash wrapper
BOOL CAutoformDecrypter::HashData(LPCTSTR cszData, LPBYTE pBuf, DWORD
dwBufSize)
{
    assert(cszData && pBuf);

    if ( !cszData || !pBuf )
    {
        m_dwLastError=E_ARG;
        return FALSE;
    }

    DoHash((LPBYTE)cszData,strlen(cszData),pBuf,dwBufSize);
    return TRUE;
}


void CAutoformDecrypter::DoHash(LPBYTE pData, DWORD dwDataSize, LPBYTE
pHash, DWORD dwHashSize)
{
    DWORD dw=dwHashSize, dw2;

    //pre-init loop
    while ( dw-->0 )
        pHash[dw]=(BYTE)dw;

    //actual hashing stuff
    while ( dwDataSize-->0 )
    {
        for ( dw=dwHashSize; dw-->0; )
        {
            //m_pPermTable = permutation table
            pHash[dw]=m_pPermTable[pHash[dw]^pData[dwDataSize]];
        }
    }
}
```

ब्राउज़र की अगली, सातवीं पीढ़ी, इस यूजर के डेटा संग्रहण तंत्र को अपनी प्राथमिक डेटा संग्रहण विधि बनाने जा रही है, जो अच्छे पुराने **संरक्षित संग्रहण** को कम करती है। कहने के लिए बेहतर है, ऑटो-फिल डेटा और पासवर्ड, अब से यहां संग्रहीत किए जाने वाले हैं।

इस तंत्र में ऐसा क्या खास और दिलचस्प है जिसने MS को इसे प्राथमिक के रूप में उपयोग करने का निर्णय लिया? ठीक है, सबसे पहले, यह एन्क्रिप्शन विचार था, जो बिल्कुल भी नया नहीं है, लेकिन फिर भी सरल और प्रतिभाशाली है, अपमान करने के लिए। विचार यह है कि एन्क्रिप्शन कीज को संग्रहीत करना बंद कर दिया जाए और जब भी आवश्यक हो, उन्हें उत्पन्न किया जाए। ऐसी चाबियों के लिए कच्चा माल HTML पृष्ठ का वेब पता होगा।

आइए देखें कि यह विचार कैसे कार्य करता है। स्वत: भरण डेटा और पासवर्ड फ़ील्ड सहेजने के लिए IE7 का सरलीकृत एल्गोरिथम (IE8 और IE9 में समान सुरक्षा योजना है) है:

1. वेब पेज का पता सहेजें। हम इस पते का उपयोग एन्क्रिप्शन कुंजी (एन्क्रिप्शनकी) के रूप में करेंगे।
2. रिकॉर्ड की प्राप्त करें। RecordKey = SHA(EncryptionKey).
3. रिकॉर्ड की की अखंडता सुनिश्चित करने के लिए रिकॉर्डकी के लिए चेकसम की गणना करें (वास्तविक डेटा की अखंडता की गारंटी DPAPI द्वारा दी जाएगी।) RecordKeyCrc = CRC (RecordKey)।
4. एन्क्रिप्शन की के साथ डेटा (पासवर्ड) एन्क्रिप्ट करें EncryptedData = DPAPI_Encrypt(Data, EncryptionKey)।
5. रजिस्ट्री में RecordKeyCrc + RecordKey + EncryptedData सहेजें।
6. एन्क्रिप्शन कुंजी को त्यागें।

मूल वेब पेज पते के बिना पासवर्ड पुनर्प्राप्त करना बहुत मुश्किल है। डिक्रिप्शन बहुत मामूली दिखता है:

1. जब मूल वेब पेज खुला होता है, तो हम उसका पता (एन्क्रिप्शनकी) लेते हैं और रिकॉर्ड की RecordKey = SHA(EncryptionKey) प्राप्त करते हैं।
2. रिकॉर्डकी का पता लगाने की कोशिश कर रहे सभी रिकॉर्ड कीज की सूची के माध्यम से ब्राउज़ करें।
3. यदि रिकॉर्डकी मिल जाती है, तो एन्क्रिप्शनकी का उपयोग करके इस की के साथ संग्रहीत डेटा को डिक्रिप्ट करें। Data = DPAPI_Decrypt(EncryptedData, EncryptionKey).

सरल लगने के बावजूद, यह वेब पासवर्ड एन्क्रिप्शन एल्गोरिथम आज के सबसे मजबूत में से एक है। हालाँकि, इसमें एक बड़ी खामी है (या लाभ, आप इसे किस तरह से देखते हैं।) यदि आप मूल वेब पेज पते को बदलते हैं या भूल जाते हैं, तो इसके लिए पासवर्ड पुनर्प्राप्त करना असंभव होगा।

2.8 कंटेंट एडवाइजर पासवर्ड

और हमारी सूची में अंतिम आइटम कन्टेन्ट एडवाइजर पासवर्ड है। कन्टेन्ट एडवाइजर को मूल रूप से कुछ वेबसाइटों तक पहुंच को प्रतिबंधित करने के लिए एक टूल के रूप में विकसित किया गया था। हालांकि, किसी कारण से यह कई यूजर्स द्वारा पसंद नहीं किया गया था (निश्चित रूप से, आप इससे असहमत हो सकते हैं।) यदि आपने एक बार कन्टेन्ट एडवाइजर चालू किया, एक पासवर्ड दर्ज किया और फिर इसे भूल गए, तो आप अधिकांश इंटरनेट वेबसाइटों तक नहीं पहुंच पाएंगे। सौभाग्य से (या दुर्भाग्य से), इसे आसानी से ठीक किया जा सकता है।

वास्तविक इंटरनेट पासवर्ड को प्लेनटेक्स्ट के रूप में संग्रहीत नहीं किया जाता है। इसके बजाय, सिस्टम अपने MD5 हैश की गणना करता है और इसे Windows रजिस्ट्री में संग्रहीत करता है। प्रतिबंधित क्षेत्र तक पहुँचने के प्रयास पर, यूजर द्वारा दर्ज किया गया पासवर्ड भी हैश किया जाता है, और प्राप्त हैश की तुलना रजिस्ट्री में संग्रहीत एक के साथ की जाती है। Passcape Internet Explorer Password Recovery स्रोत कोड जाँच कन्टेन्ट एडवाइजर पासवर्ड पर एक नज़र डालें:

```
void CContentAdvisorDlg::CheckPassword()
{
   CRegistry registry;
```

```
    //read the registry
    registry.SetKey(HKLM,
"SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Ratings");

    BYTE pKey[MD5_DIGESTSIZE], pCheck[MD5_DIGESTSIZE];
    if ( !registry.GetBinaryData("Key",pKey,MD5_DIGESTSIZE) )
    {
        MessageBox(MB_ERR,"Can't read the password.");
        return;
    }

    //Get one set by user
    CString cs;
    m_wndEditPassword.GetWindowText(cs);
    MD5Init();
    MD5Update((LPBYTE)(LPCTSTR)cs,cs.GetLength()+1);
    MD5Final(pCheck);

    //Check hashes
    if ( memcmp(pKey,pCheck,MD5_DIGESTSIZE)==0 )
        MessageBox(MB_OK,"The password is correct!");
    else
        MessageBox(MB_OK,"Wrong password.");
}
```

पहली चीज जिसके बारे में आप सोच सकते हैं, वह है ब्रूटफोर्स या शब्दकोश अटैक का उपयोग करके पासवर्ड चुनने का प्रयास करना। हालाँकि, इसका एक और अधिक सुंदर तरीका है। आप बस हैश को रजिस्ट्री से हटा सकते हैं। इतना ही; इतना आसान... ठीक है, इसके बजाय इसका नाम बदलना बेहतर है, ताकि यदि आपको कभी इसकी आवश्यकता हो, तो आप इसे वापस पुनर्स्थापित कर सकें। कुछ प्रोग्राम यूजर्स को CA पासवर्ड, "ड्रैग आउट" पासवर्ड संकेत, टॉगल पासवर्ड चालू/बंद करने आदि की भी जांच करने देते हैं।

इंटरनेट एक्सप्लोरर पासवर्ड रिकवरी सॉफ्टवेयर

3 इंटरनेट एक्सप्लोरर पासवर्ड रिकवरी सॉफ्टवेयर

यह ध्यान देने योग्य है कि सभी पासवर्ड रिकवरी प्रोग्रामों को संदेह नहीं है कि पासवर्ड रिकवर करने के कई तरीके हैं। सबसे अधिक संभावना है, यह इस तथ्य से संबंधित है कि कुछ पासवर्ड (जैसे, सिंक्रोनाइज़ेशन पासवर्ड) अक्सर वास्तविक जीवन में उपयोग नहीं किए जाते हैं, और FTP पासवर्ड इतना आसान नहीं होता है कि उन्हें 'घसीटा' जा सके। पृथ्वी पर सबसे लोकप्रिय ब्राउज़र के लिए पासवर्ड रिकवर करने के लिए सबसे लोकप्रिय कोमर्सियल प्रोडक्ट्स का संक्षिप्त विवरण यहां दिया गया है :)

एडवांस इन्टरनेट एक्सप्लोरर पासवर्ड रिकवरी - मशहूर कंपनी ElcomSoft का प्रोग्राम ऑटो-फॉर्म पासवर्ड और एन्क्रिप्टेड FTP पासवर्ड को नहीं पहचानता है। शायद, प्रोग्राम के अंतिम वर्जन ने ऐसा करना सीख लिया होगा। सरल, सुविधाजनक यूजर इंटरफेस। प्रोग्राम को स्वचालित रूप से ऑनलाइन अपग्रेड किया जा सकता है।

पास्स्वेर से इंटरनेट एक्सप्लोरर की - इसी तरह, कुछ प्रकार के पासवर्ड को नहीं पहचानता है। कभी-कभी कुछ असामान्य प्रकार के IE के URL को पढ़ते समय प्रोग्राम एक गंभीर एरर के साथ रुक जाता है। रिकवर किए जा रहे पासवर्ड के पहले दो अक्षर प्रदर्शित करता है। ध्यान देने योग्य लाभ स्पार्टन यूजर इंटरफेस और ऑपरेटिंग सुविधा हैं।

Thegrideon सॉफ़्टवेयर से इंटरनेट एक्सप्लोरर पासवर्ड - बुरा नहीं है, लेकिन केवल तीन प्रकार के इंटरनेट एक्सप्लोरर पासवर्ड रिकवर कर सकते हैं (यह अधिकांश मामलों के लिए पर्याप्त है।) FTP पासवर्ड के साथ ठीक से व्यवहार करता है। वर्जन 1.1 में ऑटोफ़ॉर्म पासवर्ड रिकवर करने में समस्याएँ हैं। सुविधाजनक यूजर इंटरफेस है, जो किसी तरह AIEPR की याद दिलाता है। कंपनी की वेबसाइट की सुंदरता और सहायकता से कोई भी पूरी तरह से अभिभूत हो सकता है।

रिक्सलर सॉफ्टवेयर से इंटरनेट पासवर्ड रिकवरी ट्रूलबॉक्स - पहले कवर किए गए प्रतिस्पर्धियों की तुलना में कुछ अधिक कार्यक्षमता प्रदान करता है। यह एन्क्रिप्टेड FTP पासवर्ड को रिकवर कर सकता है और चयनित संसाधनों को हटा सकता है। हालाँकि, इसमें कुछ प्रोग्रामिंग त्रुटियां हैं। उदाहरण के लिए, कुछ प्रकार के IE रिकॉर्ड्स को हटाया नहीं जा सकता है। कार्यक्रम एक महान, विस्तृत हेल्प फ़ाइल के साथ आता है।

ABF सॉफ्टवेयर से ABF पासवर्ड रिकवरी - अनुकूल यूजर इंटरफेस के साथ काफी अच्छा कार्यक्रम। कार्यक्रम द्वारा समर्थित IE रिकॉर्ड प्रकारों की सूची लंबी नहीं है। फिर भी, यह उन सभी के साथ ठीक से व्यवहार करता है। प्रोग्राम को बहु-कार्यात्मक के रूप में वर्गीकृत किया जा सकता है, क्योंकि यह अन्य प्रोग्रामों के लिए भी पासवर्ड को रिस्टोर कर सकता है।

यहां नामित सभी कार्यक्रमों की प्रमुख कमी केवल वर्तमान में लॉग ऑन किए गए यूजर के लिए पासवर्ड रिकवर करने की क्षमता है।

जैसा कि ऊपर कहा गया था, संग्रहीत इंटरनेट एक्सप्लोरर संसाधनों के सामान्य निकाय को एक विशेष स्टोरेज में रखा जाता है जिसे **प्रोटेक्टेड स्टोरेज** कहा जाता है। संरक्षित भंडारण विशेष रूप से व्यक्तिगत डेटा संग्रहीत करने के लिए विकसित किया गया था। इसलिए इसके साथ काम करने के लिए कार्य **PS API** कहा जाता है) डोक्युमेंटमेन्टेड नहीं हैं। संरक्षित भंडारण को पहली बार इंटरनेट एक्सप्लोरर के वर्जन 4 के रिलीज के साथ पेश किया गया था, जो कि, तीसरे वर्जन के विपरीत, जीरो से लिखा गया था।

इसलिए, हाल के समय तक, इंटरनेट एक्सप्लोरर पासवर्ड को रिकवर करने के सभी कार्यक्रमों में अनडोक्युमेंटमेन्टेड API का उपयोग किया गया था। यही कारण है कि रिकवरी कार्य पर एक महत्वपूर्ण प्रतिबंध लागू किया गया था: PS API केवल उस यूजर के लिए पासवर्ड के साथ काम कर सकता है जो वर्तमान में लॉग ऑन है। जब सिस्टम प्रोटेक्टेड स्टोरेज में संग्रहीत डेटा को एन्क्रिप्ट करता है, तो अन्य सभी चीजों के अलावा यह यूजर के SID का उपयोग करता है, जिसके बिना संग्रहीत पासवर्ड को रिकवर करने के लिए यह सचमुच असंभव है (कंप्यूटर के गणना प्रदर्शन के वर्तमान स्तर को ध्यान में रखते हुए)।

प्रोटेक्टेड स्टोरेज एक बहुत अच्छी तरह से सोचे हुए डेटा एन्क्रिप्शन विधि के माध्यम का उपयोग करता है, जो मास्टर की और मजबूत एल्गोरिदम, जैसे **des**, **sha-1**, और **sha1-hmac** का उपयोग करता है। इसी तरह की डेटा एन्क्रिप्शन विधियों का उपयोग अब अधिकांश आधुनिक ब्राउज़रों में किया जाता है; जैसे Opera या FireFox में। Microsoft, इस बीच, चुपचाप लेकिन निश्चित रूप से नए विकसित और परीक्षण करता है। जब यह लेख लिखा गया था, तो Internet Explorer 7 के प्री-बीटा वर्जन में प्रोटेक्टेड स्टोरेज का उपयोग केवल FTP पासवर्ड संग्रहीत करने के लिए किया गया था।

इस प्रारंभिक वर्जन के विश्लेषण से पता चलता है कि Microsoft नए, दिलचस्प एन्क्रिप्शन एल्गोरिदम के रूप में एक और 'आश्चर्य' तैयार कर रहा है। यह निश्चित रूप से ज्ञात नहीं है, लेकिन सबसे अधिक संभावना है कि नई कंपनी की डेटा सुरक्षा तकनीक **कार्डस्पेस** (पूर्व में **इन्फोकार्ड**) निजी डेटा के एन्क्रिप्शन में शामिल होगी।

इस प्रकार, बहुत अधिक विश्वास के साथ कोई यह दावा कर सकता है कि Windows Vista और इंटरनेट एक्सप्लोरर के 7वें वर्जन के जारी होने के साथ, पासवर्ड को मौलिक रूप से नए एल्गोरिदम के साथ संग्रहीत और एन्क्रिप्ट किया जाएगा, दिखावा, और प्रोटेक्टेड स्टोरेज इंटरफ़ेस, सभी तीसरे पक्ष के डेवलपर्स के लिए खुला हो जाएगा।

यह कुछ हद तक दुखद है, क्योंकि हमें लगता है कि प्रोटेक्टेड स्टोरेज की वास्तविक क्षमता अभी भी उजागर नहीं हुई थी। और इसलिए हम ऐसा सोचते हैं:

- सबसे पहले, प्रोटेक्टेड स्टोरेज मॉड्यूल संरचना पर आधारित है, जो अन्य स्टोरेज प्रदाताओं को इसमें प्लग करने की अनुमति देता है। हालाँकि, पिछले 10 वर्षों से जबकि प्रोटेक्टेड स्टोरेज मौजूद है, एक भी नया स्टोरेज प्रदाता नहीं बनाया गया था। सिस्टम प्रोटेक्टेड स्टोरेज ऑपरेटिंग सिस्टम में एकमात्र स्टोरेज प्रोवाइडर है, जो डिफॉल्ट रूप से उपयोग किया जाता है।
- दूसरा, प्रोटेक्टेड स्टोरेज की अपनी, अंतर्निर्मित पहुंच प्रबंधन प्रणाली है, जो किसी कारण से, इंटरनेट एक्सप्लोरर या अन्य MS उत्पादों में उपयोग नहीं की जाती है।
- तीसरा, यह बहुत स्पष्ट नहीं है कि MS ने ऑटो-कम्प्लेट डेटा और पासवर्ड संग्रहीत करने में प्रोटेक्टेड स्टोरेज को अस्वीकार करने का निर्णय क्यों लिया है। इसे एक आजमाए हुए और सच्चे डेटा स्टोरेज के रूप में अस्वीकार करें, न कि डेटा एन्क्रिप्शन तंत्र। एक नया एन्क्रिप्शन एल्गोरिथम लागू करते समय कम से कम डेटा संग्रहीत करने के लिए प्रोटेक्टेड स्टोरेज रखना अधिक तार्किक रूप से सिद्ध होगा। बिना असफलता के, उसके लिए वजनदार कारण थे। इसलिए, इस विषय पर MS विशेषज्ञों की राय सुनना दिलचस्प होगा।

PIPER - पहला परिचित

4 PIPER - पहला परिचित

पासस्केप इंटरनेट एक्सप्लोरर पासवर्ड रिकवरी को विशेष रूप से PS API के प्रतिबंध को बायपास करने और रजिस्ट्री की बाइनरी फाइलों से सीधे पासवर्ड रिकवर करना संभव बनाने के लिए विकसित किया गया था। इसके अलावा, इसमें उन्नत यूजर्स के लिए कई अतिरिक्त सुविधाएँ हैं।

प्रोग्राम का विजार्ड आपको कई ऑपरेटिंग मोड में से एक चुनने की अनुमति देता है:

ऑटोमेटिक

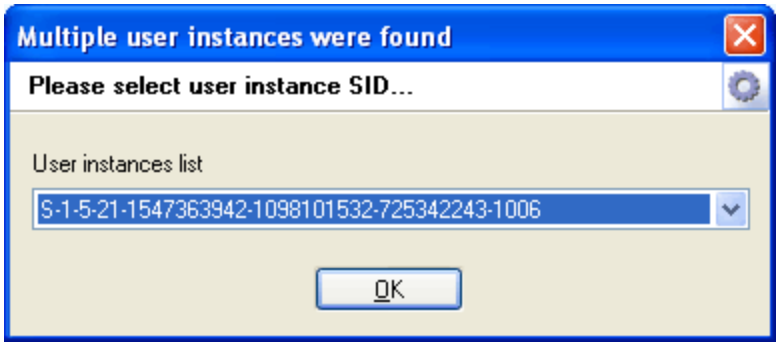
वर्तमान यूजर के पासवर्ड बंद PS API इंटरफेस तक पहुंचकर रिकवर किए जाएंगे। वर्तमान में इंटरनेट एक्सप्लोरर में संग्रहीत सभी मौजूदा यूजर के पासवर्ड माउस के एक क्लिक के साथ रिकवर किए जाएंगे।

मैनुअल

पासवर्ड PS API के बिना रिकवर किया जाएगा। इस पद्धति का मुख्य लाभ आपके पुराने विंडोज अकाउन्ट से पासवर्ड रिकवर करने की क्षमता है। उस प्रयोजन के लिए, आपको यूजर की रजिस्ट्री फ़ाइल में पाथ दर्ज करना होगा। रजिस्ट्री फ़ाइलें सामान्यतः पढ़ने के लिए उपलब्ध नहीं होती हैं; हालांकि, PIEPR में उपयोग की जाने वाली तकनीक ऐसा करने की अनुमति देती है (बशर्ते आपके पास स्थानीय एडमिनिस्ट्रेटिव अधिकार हों।)

यूजर की रजिस्ट्री फ़ाइल का नाम ntuser.dat है; यह यूजर के प्रोफाइल में रहता है, जो सामान्य रूप से %SYSTEMDRIVE%:\Documents and Settings\%USERNAME% है, जहां %SYSTEMDRIVE% ऑपरेटिंग सिस्टम के साथ सिस्टम डिस्क के लिए है, और %USERNAME% सामान्य रूप से अकाउन्ट नाम है। उदाहरण के लिए, रजिस्ट्री फ़ाइल का पथ इस तरह दिख सकता है: C:\Documents and Settings\Johnnt\user.dat

यदि आप अपने ऑपरेटिंग सिस्टम को Windows NT में अपग्रेड करने के बाद Windows 9x/ME के खुश मालिक रहे हैं, तो प्रोटेक्टेड स्टोरेज आपके पुराने निजी डेटा की एक कॉपी को सहेज लेगा। इसके परिणामस्वरूप, प्रोटेक्टेड स्टोरेज में कई यूजर पहचानकर्ता हो सकते हैं, इसलिए डेटा के डिक्रिप्शन तक पहुंचने से पहले PIEPR आपसे सही पहचानकर्ता का चयन करने के लिए कहेगा (चित्र 3)।



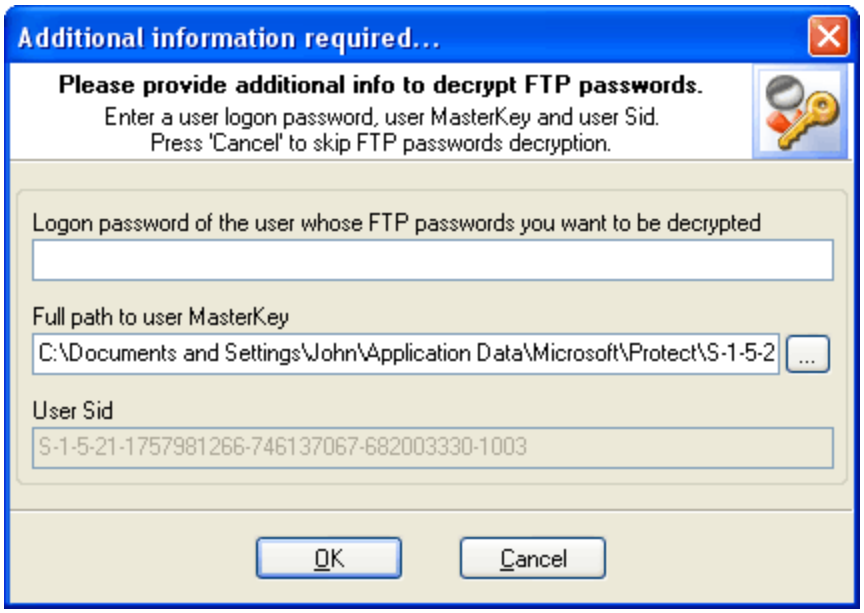
चित्र 3. संरक्षित स्टोरेज मालिक का चयन करना।

सूचीबद्ध SID में से एक में पुराने Windows 9x/ME द्वारा छोड़ा गया डेटा होगा। वह डेटा अतिरिक्त रूप से यूजर के लॉगऑन पासवर्ड के साथ एन्क्रिप्ट किया गया है, और PIEPR वर्तमान में ऐसे डेटा के डिक्रिप्शन का समर्थन नहीं करता है।

यदि ntuser.dat में एन्क्रिप्टेड पासवर्ड (जैसे, FTP साइट पासवर्ड) हैं, तो प्रोग्राम को उन्हें डिक्रिप्ट करने के लिए अतिरिक्त जानकारी की आवश्यकता होगी (चित्र 4):

- उस यूजर का लॉगऑन पासवर्ड जिसका डेटा डिक्रिप्ट किया जाना है

- यूजर के मास्टरकी का पूरा पाथ
- यूजर का SID



चित्र 4. FTP पासवर्ड के लिए DPAPI डिक्रिप्शन डायलोग।

आम तौर पर, प्रोग्राम यूजर की प्रोफ़ाइल में अंतिम दो आइटम ढूंढता है और उस डेटा को स्वचालित रूप से भर देता है। हालाँकि, यदि ntuser.dat को किसी अन्य ऑपरेटिंग सिस्टम से कॉपी किया गया था, तो आपको इसका ध्यान खुद ही रखना होगा। काम पूरा करने का सबसे आसान तरीका यूजर की मास्टर की (उनमें से कई हो सकते हैं) के साथ ntuser.dat वाले फ़ोल्डर में पूरे फ़ोल्डर की प्रतिलिपि बनाना है। मास्टर की आपके स्थानीय कंप्यूटर पर निम्न फ़ोल्डर में रहती है: %SYSTEMDRIVE%:\Documents and Settings\%USERNAME%\Application Data\Microsoft\ Protect\%UserSid%, जहां %SYSTEMDRIVE% ऑपरेटिंग सिस्टम के साथ सिस्टम डिस्क के लिए है, %USERNAME% - अकाउन्ट का नाम, %UserSid% - यूजर का SID। उदाहरण के लिए, मास्टर की वाले फ़ोल्डर का पथ निम्नानुसार दिख सकता है: C:\Documents and Settings\John\Application Data\Microsoft\Protect\ S-1-5-21-1587165142-6173081522-185545743-1003। आइए यह स्पष्ट करें कि संपूर्ण फ़ोल्डर S-1-5-21-1587165142-6173081522-185545743-1003 को कॉपी करने की अनुशंसा की जाती है, क्योंकि इसमें कई मास्टर कीज हो सकती हैं। फिर PIEPR स्वचालित रूप से सही की का चयन करेगा।

विंडोज कुछ फोल्डर को हिडन या सिस्टम के रूप में चिह्नित करता है, इसलिए वे विंडोज एक्सप्लोरर में अदृश्य हैं। उन्हें दृश्यमान बनाने के लिए, दृश्य सेटिंग में छिपी और सिस्टम ऑब्जेक्ट दिखाने में एनेबल करें या वैकल्पिक फ़ाइल प्रबंधक का उपयोग करें।

एक बार यूजर की **मास्टर की** के साथ फ़ोल्डर को ntuser.dat के साथ फ़ोल्डर में कॉपी कर लिया जाएगा, PIEPR स्वचालित रूप से आवश्यक डेटा ढूंढ लेगा, इसलिए आपको FTP पासवर्ड रिकवर करने के लिए केवल यूजर का पासवर्ड दर्ज करना होगा।

कन्टेन्ट एडवाइजर

CA पासवर्ड, जैसा कि पहले ही कहा जा चुका है, प्लेन टेक्स्ट के रूप में नहीं रखा जाता है; इसके बजाय, इसे हैश के रूप में संग्रहीत किया जाता है। CA पासवर्ड प्रबंधन डायलोग में, यह केवल हटाने के लिए पर्याप्त है (आप बाद में किसी भी समय हटाए गए पासवर्ड को रिस्टोर कर सकते हैं) या CA के साथ लॉक की गई साइटों को अनलॉक करने के लिए इस हैश को बदल सकते हैं। यदि कोई है तो PIEPR आपका पासवर्ड संकेत भी प्रदर्शित करेगा।

तारांकन पासवर्ड

PIEPR का चौथा ऑपरेटिंग मोड, जो तारांकन के पीछे छिपे इंटरनेट एक्सप्लोरर पासवर्ड को रिकवर करने की अनुमति देता है। ऐसे पासवर्ड को रिकवर करने के लिए, बस एक **** पासवर्ड के साथ आवर्धक को विंडो पर खींचें। यह उपकरण अन्य प्रोग्रामों के लिए पासवर्ड रिकवर करने की अनुमति देता है जो IE फ्रेम्स का भी उपयोग करते हैं; उदाहरण के लिए, विंडोज एक्सप्लोरर, कुछ IE -आधारित ब्राउज़र इत्यादि।

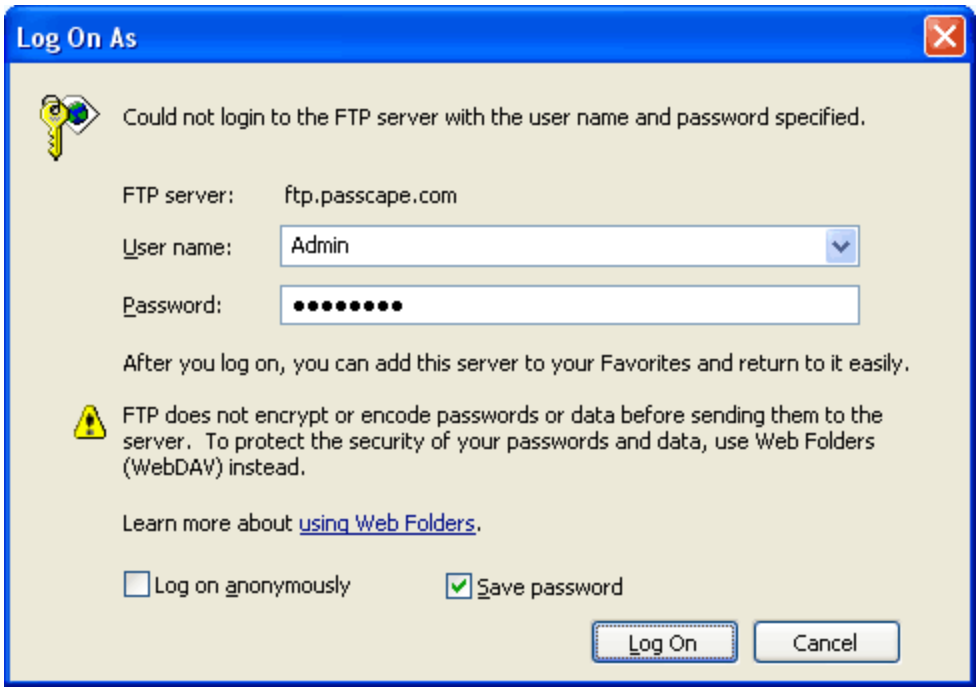
हमने बुनियादी इंटरनेट एक्सप्लोरर पासवर्ड रिकवरी मोड की समीक्षा की है। कुकीज़, कैशे, देखे गए पृष्ठों के इतिहास आदि को देखने और संपादित करने के लिए कई अतिरिक्त सुविधाएँ भी हैं। हम उन्हें विस्तार से कवर नहीं करने जा रहे हैं; इसके बजाय, हम PIEPR के साथ किए गए कुछ पासवर्ड रिकवरी उदाहरणों को देखने जा रहे हैं।

तीन वास्तविक रिकवरी उदाहरण

5 तीन वास्तविक रिकवरी उदाहरण

5.1 वर्तमान यूजर के FTP पासवर्ड पुनर्प्राप्त करना

FTP साइट खोलते समय, Internet Explorer लॉग ऑन डायलॉग को पॉप अप करता है (चित्र 5)।



चित्र 5. FTP लॉगऑन डायलोग।

यदि आपने इस साइट को खोला है और प्रमाणीकरण संवाद में 'पासवर्ड सहेजें' विकल्प सेट किया है, तो पासवर्ड को प्रोटेक्टेड स्टोरेज में सहेजा जाना चाहिए, इसलिए इसे रिकवर करना एक बहुत ही छोटा काम है। PIEPR में स्वचालित ऑपरेटिंग मोड का चयन करें और फिर 'Next' पर क्लिक करें। डिक्रिप्टेड पासवर्ड के साथ डायलोग में हमारे संसाधन का पता लगाएं जो प्रकट होता है (साइट का नाम संसाधन नाम कॉलम में दिखना चाहिए।)

जैसा कि हम देखते हैं, वर्तमान यूजर के पासवर्ड के डिक्रिप्शन से कोई विशेष कठिनाई नहीं होनी चाहिए। ओह, यदि किसी कारण से पासवर्ड नहीं मिलता है - IE की ऑटो-कम्प्लेट सेटिंग्स (चित्र 2) की जाँच करना न भूलें। संभवतः, आपने पासवर्ड सहेजने के लिए प्रोग्राम सेट नहीं किया है।

5.2 अनलोड करने योग्य ऑपरेटिंग सिस्टम से वेबसाइट पासवर्ड रिकवर करना

यह एक विशिष्ट, लेकिन घातक स्थिति नहीं है। असफल Windows रिस्टोर के बाद Internet Explorer पासवर्ड रिकवर करने की आवश्यकता उतनी ही बार होती है।

किसी भी मामले में, हमारे पास सभी फाइलों के साथ यूजर की पुरानी प्रोफ़ाइल होगी। यह सेट सामान्य रूप से काम पूरा करने के लिए पर्याप्त है। रिस्टोर के मामले में, Windows पुराने प्रोफ़ाइल को किसी भिन्न नाम से सहेजता है। उदाहरण

के लिए, यदि आपके खाते का नाम जॉन था, तो नाम बदलने के बाद यह जॉन जैसा दिख सकता है। WORK-72C39A18।

सबसे पहले और सबसे महत्वपूर्ण जो आपको करना चाहिए वह है पुरानी प्रोफ़ाइल की फ़ाइलों तक पहुँच प्राप्त करना। ऐसा करने के दो तरीके हैं:

1. एक अलग हार्ड ड्राइव पर एक नया ऑपरेटिंग सिस्टम स्थापित करें; उदाहरण के लिए, Windows XP, और पुरानी हार्ड ड्राइव को इसमें लगा दें।
2. एक Windows NT बूट डिस्क बनाएँ। ऑनलाइन उपलब्ध बूट डिस्क और यूएसबी फ्लैश डिस्क बनाने के लिए कई अलग-अलग युटिलिटीज हैं। उदाहरण के लिए, आप WinPE या BartPE का उपयोग कर सकते हैं। या एक अलग। यदि आपकी पुरानी प्रोफ़ाइल को आपकी हार्ड ड्राइव के NTFS भाग पर संग्रहीत किया गया था, तो बूट डिस्क को NTFS का सपोर्ट करना होगा।

चलो पहला रास्ता लेते हैं। एक बार जब हम पुरानी प्रोफ़ाइल तक पहुँच प्राप्त कर लेते हैं, तो हमें सिस्टम को छिपी हुई और सिस्टम फ़ाइलों को दिखाने की आवश्यकता होगी। अन्यथा, हमें जिन फ़ाइलों की आवश्यकता है वे अदृश्य हो जाएंगी। कंट्रोल पेनल खोलें, फिर फ़ोल्डर विकल्प पर क्लिक करें और फिर दृश्य टैब चुनें। इस टैब पर, 'हिडन फाइल्स एंड फोल्डर्स दिखाएं' विकल्प ढूंढें और इसे चुनें। 'सुरक्षित ऑपरेटिंग सिस्टम फ़ाइलें छुपाएं' विकल्प को साफ़ करें। जब आवश्यक पासवर्ड रिकवर हो जाते हैं, तो इन विकल्पों को उसी तरह रीसेट करना बेहतर होता है जिस तरह से उन्हें पहले सेट किया गया था।

प्रोग्राम के विजार्ड को मैनुअल मोड में खोलें और पुराने प्रोफाइल की रजिस्ट्री फाइल के लिए पाथ दर्ज करें। हमारे मामले में, वह है C:\Documents And Settings\John.WORK-72C39A18\ntuser.dat। जहां John.WORK-72C39A18 पुराने अकाउन्ट का नाम है। 'Next' पर क्लिक करें।

यह डेटा सामान्य रूप से इन्टरनेट एक्सप्लोरर पासवर्ड रिकवर करने के लिए पर्याप्त होना चाहिए। हालांकि, अगर कम से कम एक एन्क्रिप्टेड FTP पासवर्ड है, तो प्रोग्राम अतिरिक्त डेटा का अनुरोध करेगा, जिसके बिना वह इस प्रकार के पासवर्ड को रिकवर करने में सक्षम नहीं होगा (चित्र 4):

- यूजर का पासवर्ड
- यूजर की मास्टर की
- यूजर का SID.

आम तौर पर, प्रोग्राम यूजर के प्रोफ़ाइल में अंतिम दो आइटम ढूंढता है और उस डेटा को स्वचालित रूप से भर देता है। हालाँकि, अगर ऐसा नहीं हुआ, तो आप इसे हाथ से कर सकते हैं: ntuser.dat और मास्टर की वाले फ़ोल्डर को एक अलग फ़ोल्डर में कॉपी करें। संपूर्ण फ़ोल्डर को कॉपी करना महत्वपूर्ण है, क्योंकि इसमें कई कीज हो सकती हैं, और प्रोग्राम स्वचालित रूप से सही का चयन करेगा। फिर ntuser.dat फ़ाइल करने के लिए पथ दर्ज करें जिसे आपने किसी अन्य फ़ोल्डर में कॉपी किया है।

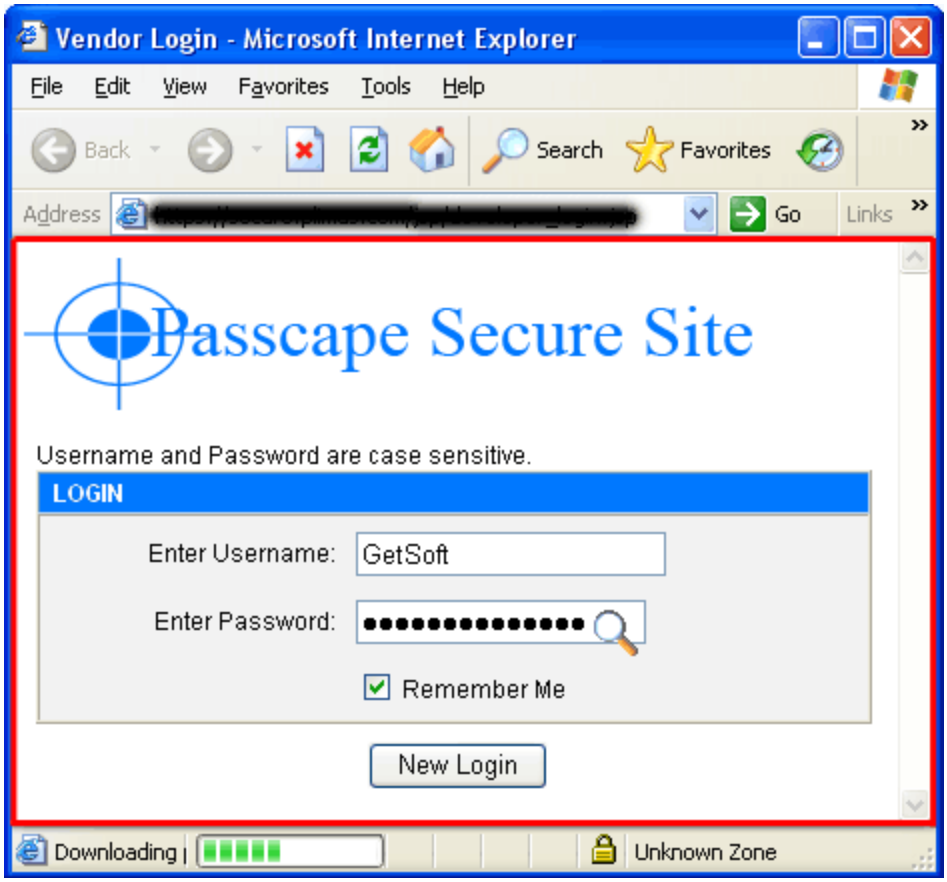
अब हमें पुराने अकाउन्ट का पासवर्ड दर्ज करना होगा, और रिकवरी पूरी हो जाएगी। यदि आप FTP पासवर्ड की परवाह नहीं करते हैं, तो आप यूजर के पासवर्ड, मास्टर की और SID एन्ट्री डायलोग को छोड़ सकते हैं।

5.3 असामान्य रूप से संग्रहीत पासवर्ड रिकवर करना

जब हम कभी-कभी ब्राउज़र में कोई वेबसाइट खोलते हैं, तो प्रमाणीकरण संवाद प्रकट होता है। हालाँकि, PIEPR इसे स्वचालित या मैन्युअल मोड में रिकवर करने में विफल रहता है। इन्टरनेट एक्सप्लोरर में 'पासवर्ड सहेजें' विकल्प सक्षम है। हमें इस पासवर्ड को रिकवर करने की आवश्यकता होगी।

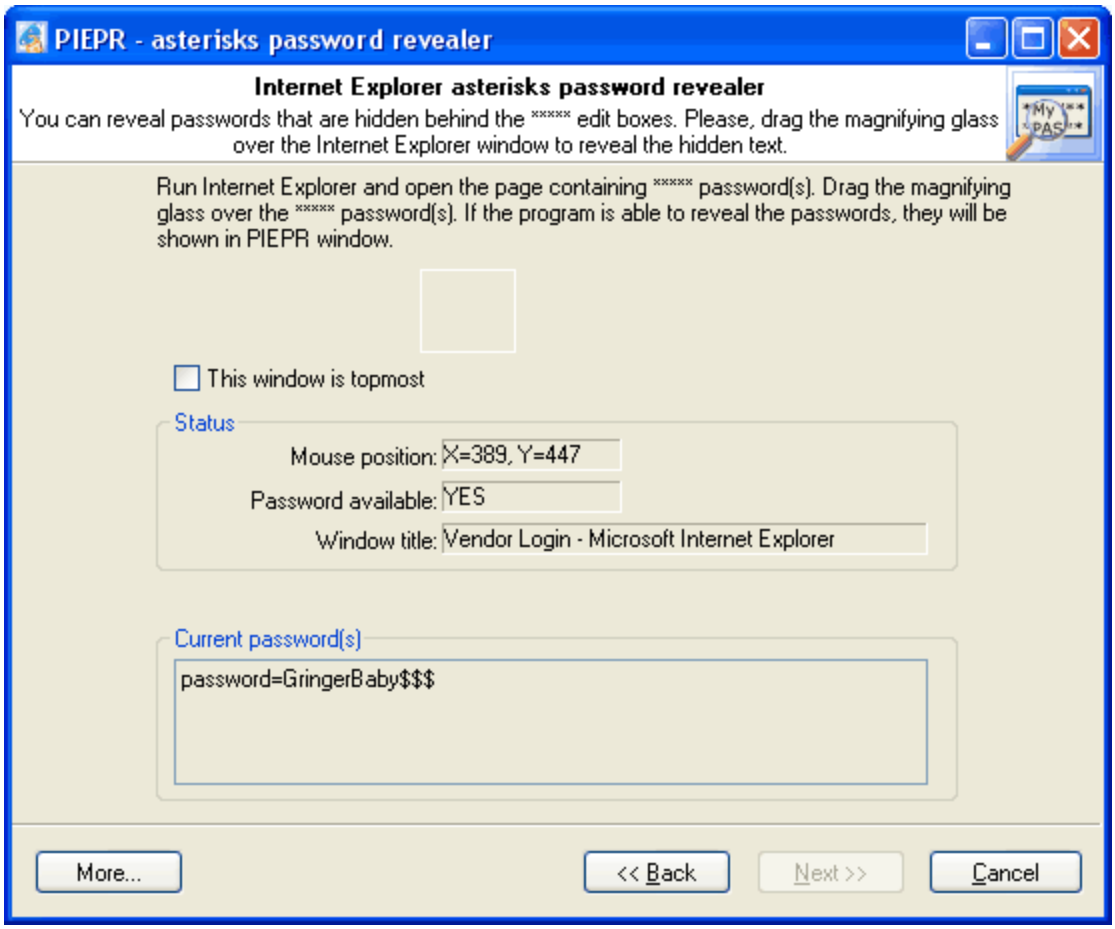
वास्तव में, कुछ वेबसाइटें ब्राउज़र को ऑटो-कम्प्लेट पासवर्ड सूची में पासवर्ड सहेजने की अनुमति नहीं देती हैं। अक्सर, ऐसी वेबसाइटें जावा में लिखी जाती हैं या वे वैकल्पिक पासवर्ड स्टोरेज विधियों का उपयोग करती हैं; उदाहरण के लिए, वे कुकीज़ में पासवर्ड स्टोर करते हैं।

यदि पासवर्ड फ़ील्ड तारक से भरा है, तो समाधान स्पष्ट है: तारक पासवर्ड ऑपरेटिंग मोड का चयन करें और फिर जादू आवर्धक संवाद खोलें। फिर बस आवर्धक को इंटरनेट एक्सप्लोरर विंडो (चित्र 6) पर खींचें।



चित्र 6. पासवर्ड तारांकन के पीछे है।

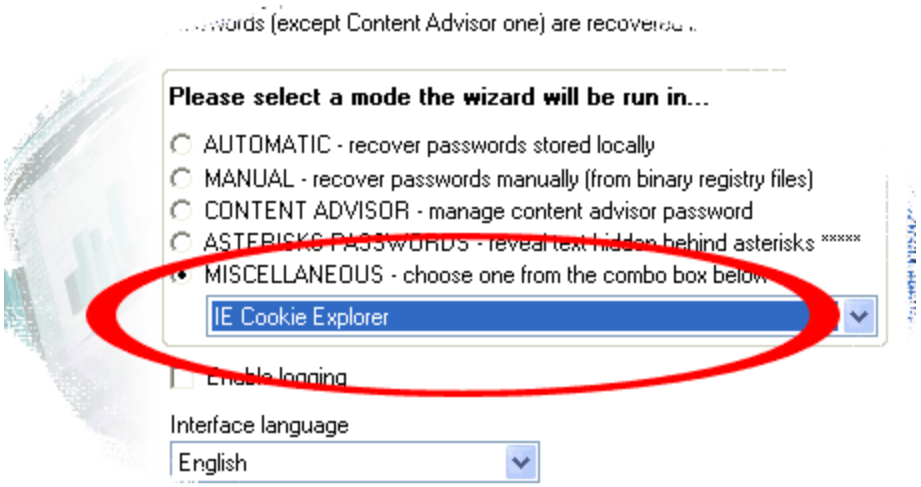
पासवर्ड (पासवर्ड, यदि इंटरनेट एक्सप्लोरर विंडो में तारक के साथ कई फ़ील्ड हैं) को PIEPR विंडो (चित्र 7) में दिखाना है।



चित्रा 7. उपयोग में आवर्धक कांच।

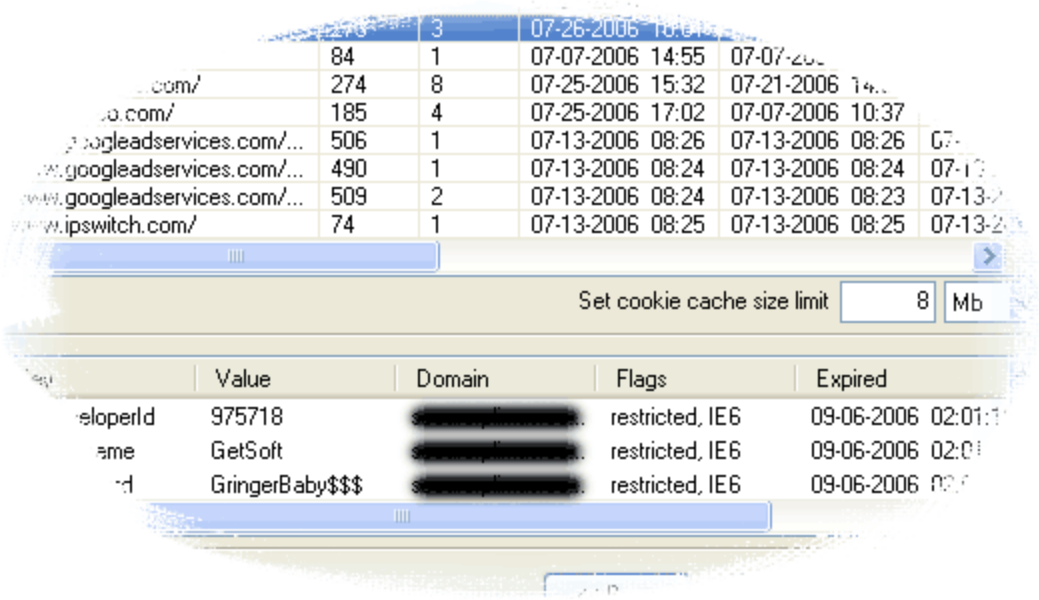
लेकिन यह हमेशा इतना आसान नहीं होता है। पासवर्ड फ़ील्ड खाली हो सकता है या उस फ़ील्ड में वास्तव में ***** हो सकता है। इस मामले में, जैसा कि आप अब तक अनुमान लगा चुके हैं, तारक पासवर्ड उपकरण बेकार हो जाएगा।

हम मान सकते हैं, पासवर्ड कुकीज़ में संग्रहीत है। आइए इसे खोजने का प्रयास करें। IE कुकी एक्सप्लोरर टूल चुनें (चित्र 8) ।



चित्र 8. IE कुकी एक्सप्लोरर।

दिखाई देने वाला डायलोग उन वेबसाइटों को सूचीबद्ध करेगा जो आपके कंप्यूटर पर कुकीज़ संग्रहीत करती हैं। वेबसाइटों की सूची को वर्णानुक्रम में क्रमबद्ध करने के लिए URL कॉलम हेडर पर क्लिक करें। इससे हमें सही वेबसाइट खोजने में आसानी होगी। वेबसाइटों की सूची के माध्यम से जाए और हमें जो चाहिए उसे चुनें। नीचे दी गई सूची इस वेबसाइट के लिए डिक्रिप्टेड कुकीज़ प्रदर्शित करेगी (चित्र 9)।



चित्र 9. डिक्रिप्टेड कुकीज़।

जैसा कि चित्र से पता चलता है, हमारे मामले में लॉगिन और पासवर्ड एन्क्रिप्टेड नहीं हैं और प्लेन टेक्स्ट के रूप में संग्रहीत हैं।

कुकीज़ अक्सर एन्क्रिप्ट की जाती हैं। इस मामले में, आपको पासवर्ड रिकवर करने में सफल होने की संभावना नहीं है। पुराने अकाउन्ट को रिकवर करने के लिए केवल एक चीज जो आप करने का प्रयास कर सकते हैं, वह है एक नया अकाउन्ट

बनाना। तब आप पुराने कुकीज़ को टेक्स्ट एडिटर में कॉपी कर सकेंगे और उन्हें नए के साथ बदल सकेंगे। हालांकि, यह तभी अच्छा होता है जब सबसे खराब आता है; इसे सामान्य रूप से उपयोग करने की अनुशंसा नहीं की जाती है।

यह भी न भूलें कि पासवर्ड वाले लगभग सभी पृष्ठों और प्रपत्रों में 'पासवर्ड भूल गए' बटन होता है।

निष्कर्ष

6 निष्कर्ष

जैसा कि यह लेख दिखाता है, इंटरनेट एक्सप्लोरर पासवर्ड रिकवर करना एक बहुत ही सरल काम है, जिसके लिए किसी विशेष ज्ञान या कौशल की आवश्यकता नहीं होती है। हालांकि, प्रतीत होने वाली सादगी के बावजूद, पासवर्ड एन्क्रिप्शन योजनाओं और एल्गोरिदम को बहुत अच्छी तरह से सोचा जाता है और साथ ही साथ लागू भी किया जाता है। हालांकि प्रोटेक्टेड स्टोरेज अवधारणा 10 वर्ष से अधिक पुरानी है, यह मत भूलो कि इसने विशेषज्ञों की सबसे अच्छी सिफारिशों को साबित कर दिया है और इस लोकप्रिय ब्राउज़र की तीन पीढ़ियों के माध्यम से लागू किया गया है।

IE के अगले, 7वें वर्जन के जारी होने के साथ, Microsoft हमारे निजी डेटा की सुरक्षा के लिए मौलिक रूप से नई योजनाएँ तैयार कर रहा है, जहाँ यह बेहतर एन्क्रिप्शन एल्गोरिदम का उपयोग करता है और प्रोटेक्टेड स्टोरेज के लिए अजीबोगरीब कमी को समाप्त करता है।

विशेष रूप से, इंटरनेट एक्सप्लोरर 7 के प्रारंभिक बीटा वर्जनो के विश्लेषण से पता चला है कि ऑटोफॉर्म पासवर्ड एन्क्रिप्शन की अब डेटा के साथ संग्रहीत नहीं हैं। वे संग्रहीत नहीं हैं, अवधि! यह एक छोटी सी जानकारी है, जिसका अनुमान पेशेवरों और अंतिम यूजर्स दोनों द्वारा इसके वास्तविक मूल्य पर लगाया जाना है, जो अंततः, वैसे भी इसका लाभ उठाएंगे।

लेकिन मुख्य बात यह है कि नई अवधारणा के जारी होने से प्रोटेक्टेड स्टोरेज की बड़ी खामी खत्म हो जाएगी, जो कि अतिरिक्त जानकारी को जाने बिना पासवर्ड को रिकवर करने की संभावना है। कहने के लिए बेहतर, एक संभावित हैकर के लिए पासवर्ड और यूजर के अन्य निजी डेटा को चोरी या क्षति पहुंचाने के लिए हार्ड ड्राइव की सामग्री तक भौतिक पहुंच प्राप्त करने के लिए पर्याप्त था। इंटरनेट एक्सप्लोरर 7 के जारी होने से स्थिति कुछ हद तक बदल जाएगी।

इस बीच, हमें इस लोकप्रिय ब्राउज़र की अगली पीढ़ी में उपयोग किए जाने वाले नए एन्क्रिप्शन तंत्र पर करीब से नज़र डालने के लिए केवल Windows Vista और IE 7 के आगमन के लिए बेसब्री से इंतजार करना होगा।