Recovering Internet Explorer passwords: theory and practice

Passcape Software

1. 介绍 3
2. Internet Explorer中存储的密码类型 3
2.1 互联网证书 3
2.2 自动填写数据 4
2.3 自动补全密码 5
2.4 FTP证书 6
2.5 同步密码 6
2.6 身份认证密码 7
2.7 AutoForms数据 7
2.8 内容审查程序密码 9
3. Internet Explorer密码恢复软件 10
4. PIEPR--初识 12
5. 三个现实生活中的恢复案例 14
5.1 恢复当前用户的FTP密码 14
5.2 从无法加载的操作系统中恢复网站密码 14
5.3 恢复不常用的存储密码 15
6. 总结 18

1 介绍

没有人可能会质疑IE浏览器是当今最流行的网络浏览器这一事实。据统计，大约70%的在线用户只喜欢使用这个程序。关于它的优点和缺点的争论可能会永远持续下去；但是，这个浏览器是其行业的领导者，这是一个不需要证明的事实。IE浏览器拥有多项内置技术，旨在使普通用户的生活更加轻松。其中一项技术--IntelliSense--是用来处理常规任务的，如自动完成访问的网页地址、自动填写表格字段、用户密码等。

今天的许多网站都需要注册，这意味着，用户必须输入用户名和密码。如果你使用的这类网站超过一打，你很可能需要一个密码管理器。所有现代浏览器都有一个内置的密码管理器，IE浏览器也不例外。事实上，如果密码很快就会被遗忘，为什么还要记住另一个密码呢？让浏览器为你完成记忆和存储密码的常规工作要容易得多。这既方便又舒适。

这将是一个完全完美的解决方案；然而，如果你的Windows操作系统崩溃了，或者重新安装的方式与它应该重新安装的方式不同，你可以很容易地丢失整个宝贵的密码列表。这就是舒适和便利的代价。好在几乎每个网站都有一个保存 "我忘记密码 "的按钮。然而，这个按钮并不总是能让你头疼。

每个软件开发商都以自己的方式解决忘记密码的恢复问题。他们中的一些人正式建议将几个重要文件复制到另一个文件夹，而另一些人则向所有注册用户发送一个特殊的工具，允许管理私人数据的迁移，第三种人则假装他们没有看到这个问题。尽管如此，需求创造了报价，目前对密码恢复程序的需求很大。

在这篇文章中，让我们尝试对存储在Internet Explorer中的私人数据类型进行分类，看看恢复数据的程序，并研究恢复丢失的互联网密码的真实案例。

2 Internet Explorer中存储的密码类型

Internet Explorer可能会存储以下类型的密码：

- 互联网凭证
- 自动完成的数据
- 自动完成的密码
- FTP凭证
- 缓存网站的同步密码
- 个人身份密码
- 自动表格数据
- 内容审查程序密码

让我们仔细看看每个列出的项目。

2.1 互联网证书

互联网凭证是指访问某些网站所需的用户登录名和密码，由wininet.dll库处理。例如，当你试图进入一个网站的保护区域时，你可能会看到以下用户名和密码提示（图1）。

图1. 互联网凭证对话框。

如果在该提示中选择了 "记住我的密码 "的选项，用户凭证将被保存在你的本地计算机上。旧版本的Windows 9x将该数据存储在用户的PWL文件中; Windows 2000和新版本将其存储在受保护的存储器中。

USERNAME.PWL（其中USERNAME是你的登录名）是一个PassWord List文件。它记录了网络上资源的密码，并利用这些密码重新连接到这些资源，这样你就不必再输入密码了。

保护性存储为应用程序提供了一个接口，以存储必须保持安全或不被修改的用户数据。存储的数据单位被称为项目。存储数据的结构和内容对保护性存储系统来说是不透明的。对项目的访问需要根据用户定义的安全样式进行确认，该样式规定了访问数据需要的确认，如是否需要密码。此外，对项目的访问受制于一个访问规则集。每个访问模式都有一个访问规则：例如，读/写。访问规则集是由访问条款组成的。通常在应用程序设置时，会提供一种机制，允许新的应用程序向用户请求访问可能由另一个应用程序创建的项目。
项目是由键、类型、子类型和名称的组合来唯一识别的。键是一个常数，指定该项目是全局的还是只与该用户相关的。名称是一个字符串，通常由用户选择。类型和子类型是GUID，通常由应用程序指定。关于类型和子类型的其他信息被保存在系统注册表中，包括诸如显示名称和用户界面提示等属性。对于子类型，父类型是固定的，作为一个属性包含在系统注册表中。类型组项目被用于一个共同的目的：例如，支付或识别。子类型组项目共享一个共同的数据格式。
我们将在接下来的一篇文章中尝试介绍保护性存储结构。

2.2 自动填写数据

自动填写数据（密码将进一步介绍）也存储在保护存储中，并以HTML表格字段名和相应的用户数据的列表形式出现。例如，如果一个HTML页面包含一个电子邮件地址输入对话框：一旦用户输入了他的电子邮件地址，受保护的存储空间将有HTML字段名，地址值，以及记录最后被访问的时间。

而HTML页面的标题和网站地址则不被存储。这是好还是坏？这很难确定；好的可能性多于坏的。这里有明显的优点：它节省了自由空间，加快了浏览器的性能。如果你认为最后一条无关紧要，请试着想象一下，在一个几千人的（这种情况并不像看起来那么罕见）自动填充列表中，你将不得不执行几个额外的检查。

另一个明显的好处是，相同的按名称（通常是按主题）的HTML表单字段的数据将被存储在同一个地方，共同的数据将被用于此类页面的自动填充。我们将通过这个例子看到这一点。如果一个HTML页面包含一个名称为 "email "的自动填充字段，并且用户在该字段中输入了他的电子邮件地址，IE将在存储区中放入大致的 "email=my@email.com"。从现在开始，如果用户打开另一个网站，其中有一个页面有相同的字段名称 "电子邮件"，用户将被建议用他在第一个页面上输入的值来自动填写（my@email.com）。因此，浏览器在某种程度上发现了自身的AI能力。

这种数据存储方法的主要缺点来自于我们刚才描述的优点。想象一下，用户在一个网页上输入了自动填充的数据。如果有人知道HTML表格的字段名，这个人就可以用相同的字段名创建他自己最简单的HTML页面，并从本地磁盘打开。为了发现在这个字段中输入的数据，这个人甚至不需要连接到互联网并打开原始的WWW地址。

2.3 自动补全密码

然而，在有密码数据的情况下，正如你可能已经猜到的，数据不会被自动填入。因为自动完成的密码是和网页名称一起存储的，而且每个密码只与一个特定的HTML网页绑定。

在新的版本中，Internet Explorer 7，自动完成密码和数据的加密方式都完全不同；新的加密方式没有刚才所说的缺点（如果这可以归为缺点的话。）

值得注意的是，Internet Explorer允许用户通过选项菜单手动管理自动填充参数（图2）。

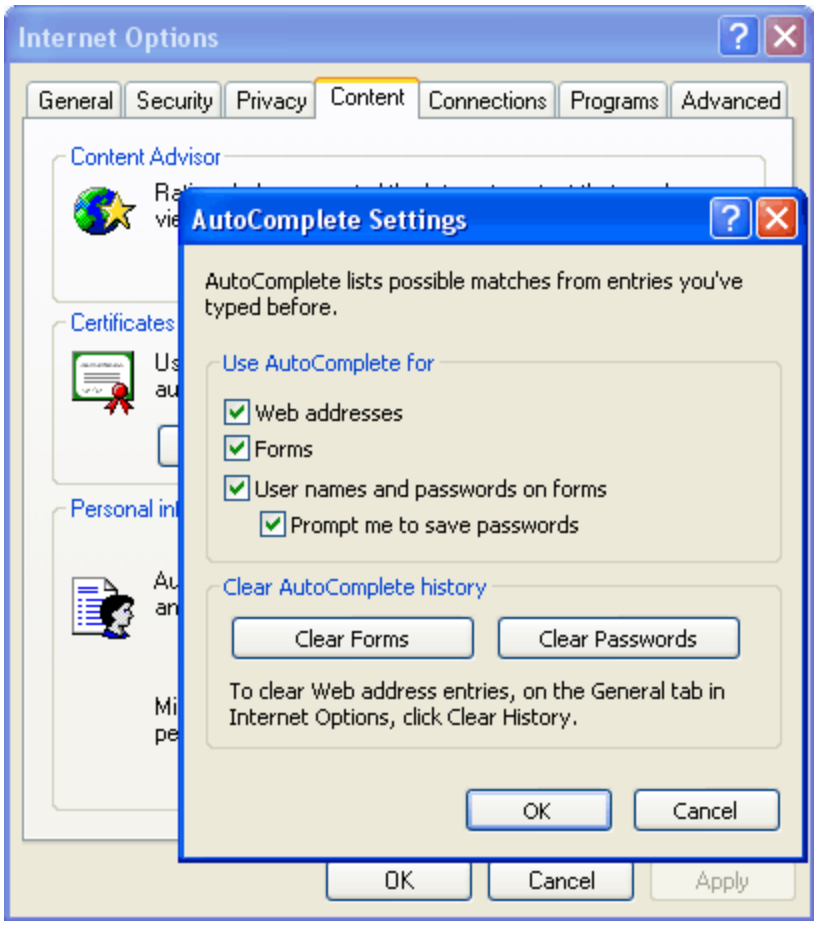

图2. Internet Explorer的自动完成设置。

2.4 FTP证书

FTP站点的凭证也是以同样的方式存储的。值得注意的是，从Windows XP开始，FTP密码还用DPAPI 进行了加密.。这种加密方法使用登录密码。自然，这使得手动恢复这种丢失的密码变得更加困难，因为现在需要有用户的主密钥、SID和账户密码。

2.5 同步密码

同步密码使用户不必为缓存网站（设置为离线的网站）输入密码。这种类型的密码也存储在IE的保护存储中。

2.6 身份认证密码

身份密码也是如此。基于身份的访问管理机制在微软的产品中并不普遍，也许除了Outlook Express。

2.7 AutoForms数据

有一个特别的段落必须涵盖表格自动填写方法，它构成了一种存储数据的混合方式。这种方法将实际数据存储在受保护的存储器中，而数据所属的URL则存储在用户的注册表中。写在注册表中的URL不是以明文形式存储的，而是以哈希形式存储的。下面是Internet Explorer 4-6中读取表单自动填充数据的算法：

```
//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]];
      }
    }
}
```

下一代，也就是第七代浏览器，很可能会把这个用户的数据存储机制作为其主要的数据存储方式，取消了良好的老式保护存储。更好的说法是，自动填充数据和密码，从现在开始，将被存储在这里。

这个机制有什么特别之处和有趣之处，使MS决定将其作为主要存储方式？嗯，首先，是加密的想法，这一点也不新鲜，但仍然简单而天才，让人不齿。这个想法是放弃存储加密密钥，并在必要时生成它们。这种密钥的原材料是HTML页面的网址。

让我们看看这个想法是如何运作的。这里是IE7的简化算法（IE8和IE9有相同的保护方案），用于保存自动填充数据和密码字段。

1. 保存网页的地址。我们将使用这个地址作为加密密钥（EncryptionKey）。
2. 获得记录密钥。RecordKey = SHA(EncryptionKey)。
3. 计算RecordKey的校验和，以确保记录密钥的完整性（实际数据的完整性将由DPAPI保证。）RecordKeyCrc = CRC(RecordKey)。
4. 用加密密钥对数据（密码）进行加密 EncryptedData = DPAPI_Encrypt(Data, EncryptionKey).
5. 在注册表中保存RecordKeyCrc + RecordKey + EncryptedData。
6. 丢弃EncryptionKey。

如果没有原始网页地址，要恢复密码是非常非常困难的。解密看起来非常微不足道：

1. 当原始网页被打开时，我们取其地址（EncryptionKey）并获得记录密钥 RecordKey = SHA(EncryptionKey)。
2. 浏览所有记录密钥的列表，试图找到RecordKey。
3. 如果找到了RecordKey，使用EncryptionKey解密与此密钥一起存储的数据。Data = DPAPI_Decrypt(EncryptedData, EncryptionKey).

尽管看起来很简单，这种网络密码加密算法是当今最强大的算法之一。然而，它有一个主要的缺点（或优势，取决于你怎么看它）。如果你改变或忘记了原始的网页地址，就不可能恢复它的密码。

2.8 内容审查程序密码

而我们清单上的最后一项是内容审查程序密码。内容顾问最初是作为一个限制访问某些网站的工具而开发的。然而，由于某些原因，它不被许多用户所喜爱（当然，你可能不同意这一点。）如果你一旦打开了内容顾问，输入了一个密码，然后忘记了，你将无法访问互联网上的大多数网站。幸运的是（或不幸的是），这可以很容易地解决。

实际的 "内容顾问 "密码不以明文形式存储。相反，系统会计算其MD5哈希值并将其存储在Windows注册表中。在试图访问限制区时，用户输入的密码也会被哈希化，获得的哈希值会与存储在注册表中的哈希值进行比较。请看一下 Passcape Internet Explorer Password Recovery 源代码检查内容审查程序密码：

```
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.");
}
```

你可能想到的第一件事是试图通过使用蛮力或字典攻击来挑选密码。然而，有一个更优雅的方法。你可以简单地从注册表中删除哈希值。就这样，如此简单..... 好吧，最好改成重命名，这样，如果你需要它，你可以把它恢复过来。一些程序还可以让用户检查CA密码，"拖出 "密码提示，切换密码开/关，等等。

3 Internet Explorer密码恢复软件

值得注意的是，并不是所有的密码恢复程序都怀疑有这么多恢复密码的方法。最有可能的是，这与一些密码（如同步密码）在现实生活中不经常使用有关，而FTP密码也不是那么简单就能被 "拖出来"的。下面是对地球上最流行的浏览器恢复密码的最流行的商业产品的简要介绍 :)

Advanced Internet Explorer Password Recovery ElcomSoft是一家知名公司，它不识别自动格式密码和加密的FTP密码。不排除在外，程序的最新版本可能已经学会了这样做。简单、方便的用户界面。程序可以自动在线升级。

Internet Explorer Key from PassWare - 同样，也不能识别某些类型的密码。在读取某些不常见类型的IE的URL时，程序有时会出现严重错误。显示正在恢复的密码的前两个字符。值得注意的优点是简洁的用户界面和操作方便。

Internet Explorer Password from Thegrideon Software - 不错，但只能恢复三种Internet Explorer的密码（这对大多数情况来说已经足够了）。 正确处理FTP密码。1.1版在恢复AutoForm密码时有问题。具有方便的用户界面，这在某种程度上使人想起了AIEPR。该公司网站的美感和帮助性可以让人完全折服。

Internet Password Recovery Toolbox from Rixler Software - 与之前涉及的竞争对手相比，它提供了一些更大的功能。它可以恢复加密的FTP密码和删除选定的资源。然而，它有一些编程错误。例如，某些类型的IE记录不能被删除。该程序带有一个很好的、详细的帮助文件。

ABF Password Recovery from ABF software - 这是一个相当好的程序，用户界面友好。该程序所支持的IE记录类型列表并不长。不过，它能正确处理所有这些记录。该程序可以归类为多功能程序，因为它也可以恢复其他程序的密码。

这里提到的所有程序的主要缺点是只能恢复当前登录的用户的密码。

如上所述，Internet Explorer的总体资源被保存在一个名为"保护存储器"的特殊存储器中。保护存储"是专门为存储个人数据而开发的。因此，使用它的功能（称为PS API）并没有被记录下来。保护存储是随着Internet Explorer第四版的发布而首次引入的，顺便说一下，与第三版不同，它是从头开始编写的。

所以，直到最近，所有恢复IE密码的程序都使用了这些没有记录的API。这就是为什么对恢复工作有一个重要限制的原因。PS API只能处理当前登录的用户的密码。当系统对存储在保护存储器中的数据进行加密时，除了使用其他东西外，还使用了用户的SID，如果没有这个SID，要恢复存储的密码简直是不可能的（考虑到目前计算机的计算性能水平）。

保护存储"使用了一种经过深思熟虑的数据加密方法，它使用主密钥和强大的算法，如des、sha-1和sha1-hmac。类似的数据加密方法现在在大多数现代浏览器中使用；例如，在Opera或FireFox中。与此同时，微软也在悄悄地但肯定地开发和测试新的方法。写这篇文章的时候，在Internet Explorer 7的前Beta版本中，保护存储只用于存储FTP密码。

对这个初步版本的分析表明，微软正在准备另一个"惊喜"，即新的、有趣的加密算法。目前还不清楚，但很可能新公司的数据保护技术CardSpace（原InfoCard）将参与私人数据的加密。

因此，人们可以非常自信地断言，随着Windows Vista和第七版IE浏览器的发布，密码将以根本性的新算法进行存储和加密，而保护存储界面，从表面上看，将对第三方开发者开放。

这多少有些令人难过，因为我们该为保护存储的真正潜力未被发掘出来。而这就是我们这样认为的原因：

- 首先，保护性存储是基于模块结构的，它允许将其他存储供应商插入其中。然而，在过去的10年里，当保护存储存在时，没有一个新的存储提供者被创建。系统保护存储是操作系统中唯一的存储提供者，它被默认使用。
- 第二，"保护存储"有它自己的、内置的访问管理系统，由于某种原因，它没有被用于Internet Explorer或其他MS产品中。
- 第三，不很清楚为什么MS决定在存储自动完成数据和密码时拒绝保护存储。拒绝它作为一种久经考验的数据存储，而不是数据加密机制。在实施新的加密算法时，至少要保留保护性存储来存储数据，这在逻辑上会更有说服力。无独有偶，这其中也有重量级的原因。因此，听听MS专家对这个问题的看法是很有意思的。

4 PIEPR--初识

Passcape Internet Explorer Password Recovery 专门为绕过PS API的限制而开发，并使其能够从注册表的二进制文件中直接恢复密码。此外，它还为高级用户提供了一些附加功能。

程序向导允许您选择几种操作模式之一：

Automatic
当前用户的密码将通过访问关闭的PS API接口恢复。只需单击鼠标即可恢复当前存储在Internet Explorer中的所有当前用户密码。

Manual
密码将在没有PS API的情况下恢复。此方法的主要优点是能够从旧Windows帐户恢复密码。为此，您需要输入用户注册表文件的路径。注册表文件通常不可读取；但是，PIEPR中使用的技术允许这样做（前提是您拥有本地管理权限）

用户的注册表文件名为ntuser。dat；它位于用户的配置文件中，通常为%SYSTEMDRIVE%:\Documents and Settings\%USERNAME%，其中%SYSTEMDRIVE%代表操作系统的系统磁盘，%USERNAME%通常是帐户名。例如，注册表文件的路径可能如下所示：C:\Documents and Settings\johnt\user.dat

如果您曾经是Windows 9x/ME的快乐拥有者，在您将操作系统升级到Windows NT之后，受保护的存储将为您节省一份旧的私人数据副本。因此，受保护的存储可能包含多个用户标识符，因此PIEPR将要求您在解密数据之前选择正确的标识符（图3）。

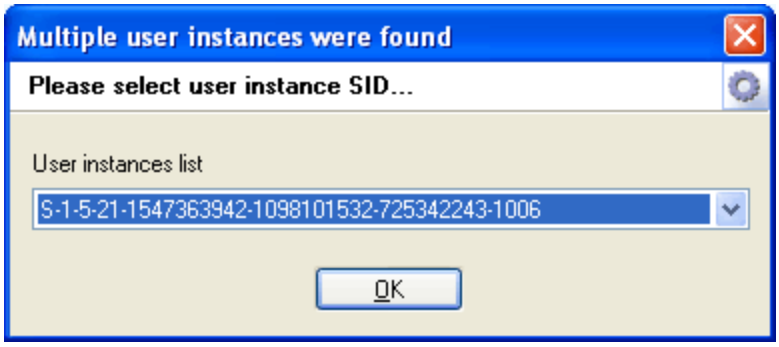

图3.选择受保护的存储所有者。

其中一个列出的SID将包含旧Windows 9x/ME留下的数据。该数据还使用用户的登录密码进行加密，PIEPR目前不支持此类数据的解密。

如果是ntuser。dat包含加密密码（如FTP站点密码），程序需要额外的信息才能解密它们（图4）：
- 数据要被解密的用户的登录密码
- 用户主密钥的完整路径
- 用户的SID

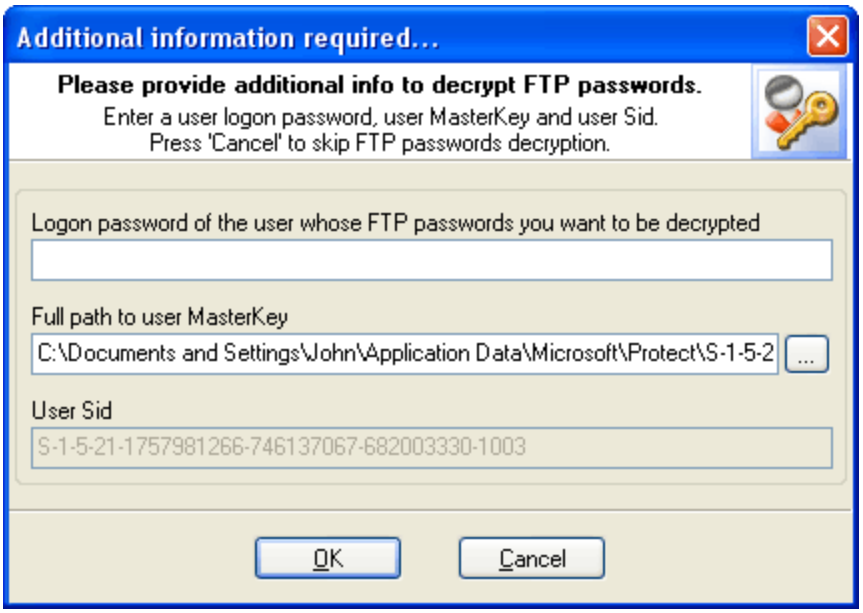

图4. FTP密码的DPAPI解密对话框。

通常情况下，程序会找到用户资料中的最后两项，并自动填充这些数据。但是，如果ntuser.dat是从另一个操作系统复制过来的，你就必须自己处理这个问题。最简单的方法是把装有用户主密钥的整个文件夹（可能有几个）复制到装有ntuser.dat的文件夹。主密钥驻留在本地计算机的以下文件夹中：%SYSTEMDRIVE%:\Documents and Settings\%USERNAME%\Application Data\Microsoft\Protect\%UserSid%，其中%SYSTEMDRIVE%代表操作系统的系统盘，%USERNAME%-账户名，%UserSid%-用户的SID。例如，带有主密钥的文件夹的路径可能看起来如下。C:\Documents and Settings\John\Application Data\MicrosoftProtect\S-5-21-1587165142-6173081522-185545743-1003。让我们明确一下，建议复制整个文件夹S-1-5-21-1587165142-6173081522-185545743-1003，因为它可能包含几个主密钥。然后PIEPR会自动选择正确的密钥。

Windows将一些文件夹标记为隐藏或系统，所以它们在Windows Explorer中是不可见的。要使它们可见，请在视图设置中启用显示隐藏和系统对象，或使用其他文件管理器。

一旦装有用户主密钥的文件夹被复制到装有ntuser.dat的文件夹中，PIEPR将自动找到所需的数据，所以你只需要输入用户的密码来恢复FTP密码。

Content Advisor

如之前所述，CA密码不是以纯文本形式保存的，而是以哈希值形式保存的。在CA密码管理对话框中，只需删除（以后可以随时恢复被删除的密码）或改变这个哈希值就可以解锁用CA锁定的网站。如果有密码提示，PIEPR也会显示你的密码提示。

Asterisks passwords

PIEPR的第四种操作模式，可以恢复隐藏在星号后面的Internet Explorer密码。要恢复这样的密码，只需将放大镜拖到有密码的窗口****。这个工具也可以恢复其他使用IE框架的程序的密码；例如，Windows Explorer，一些基于IE的浏览器等。

我们已经审查了基本的Internet Explorer密码恢复模式。还有一些额外的功能，用于查看和编辑cookies、缓存、访问过的网页历史记录等。我们不打算详细介绍这些功能；相反，我们要看一些用PIEPR完成的密码恢复例子。

5 三个现实生活中的恢复案例

5.1 恢复当前用户的FTP密码

当打开一个FTP站点时，Internet Explorer会弹出登录对话框（图5）。

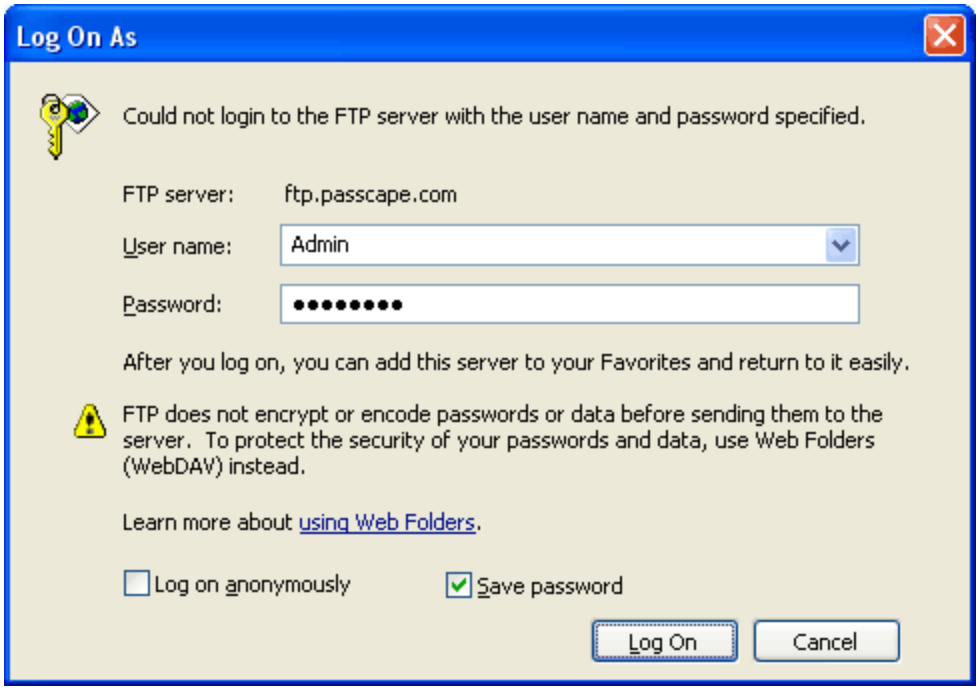

图5. FTP登录对话框。

如果你已经打开了这个网站，并在认证对话框中设置了'保存密码'选项，那么密码必须保存在受保护的存储器中，所以恢复密码是一个相当琐碎的工作。在PIEPR中选择自动操作模式，然后点击'下一步'。在出现的解密密码对话框中找到我们的资源（网站名称必须出现在资源名称栏中。）

正如我们所看到的，对当前用户密码的解密不应造成任何特殊困难。哦，如果由于某种原因找不到密码--别忘了检查IE的自动完成设置（图2）。有可能，你根本没有将程序设置为保存密码。

5.2 从无法加载的操作系统中恢复网站密码

这是一种典型的，但不是致命的情况。在不成功的Windows重装后，需要恢复Internet Explorer密码的情况也经常发生。

在这两种情况下，我们都会有用户的旧配置文件和其中的所有文件。这套文件通常足以完成工作。在重装的情况下，Windows会将旧的配置文件保存在一个不同的名称下。例如，如果你的账户名是John，重命名后它可能看起来像John.WORK-72C39A18。

你必须做的第一件事，也是最重要的一件事，就是访问旧配置文件中的文件。有两种方法可以做到这一点：

1. 在不同的硬盘上安装一个新的操作系统；例如，Windows XP，并将旧的硬盘挂到它上面。
2. 创建一个Windows NT启动盘。网上有许多创建启动盘和USB闪存盘的不同工具。例如，你可以使用WinPE或BartPE。或者换一个。如果你的旧资料存储在硬盘的NTFS部分，那么启动盘就必须支持NTFS。

让我们采取第一条路线。一旦我们获得对旧配置文件的访问权，我们将需要让系统显示隐藏文件和系统文件。否则，我们需要的文件将是不可见的。打开控制面板，然后点击文件夹选项，然后选择查看选项卡。在这个选项卡上，找到 "显示隐藏的文件和文件夹 "选项并选择它。清除 "隐藏受保护的操作系统文件 "的选项。当必要的密码恢复后，最好将这些选项重置为之前的设置方式。

在手动模式下打开程序的向导，并输入旧配置文件的注册表文件的路径。在我们的例子中，那就是C:\Documents And Settings\John.WORK-72C39A18\ntuser.dat。其中John.WORK-72C39A18是旧账户名称。点击 "下一步"。

这些数据通常应该足以恢复Internet Explorer的密码。然而，如果至少有一个加密的FTP密码，该程序将要求提供额外的数据，没有这些数据，它将无法恢复此类密码（图4）：

- 用户的密码
- 用户的主密钥
- 用户的SID

通常情况下，程序会找到用户资料中的最后两项，并自动填充这些数据。然而，如果这没有发生，你可以用手来做：把ntuser.dat和装有主密钥的文件夹复制到一个单独的文件夹。复制整个文件夹很重要，因为它可能包含几个密钥，程序会自动选择正确的一个。然后输入复制到另一个文件夹的文件ntuser.dat的路径。

现在我们需要输入旧账户密码，恢复工作就完成了。如果你不关心FTP密码，你可以跳过用户密码、主密钥和SID输入对话框。

5.3 恢复不常用的存储密码

当我们有时在浏览器中打开一个网站时，会出现认证对话框。然而，PIEPR在自动或手动模式下都无法恢复。Internet Explorer中的 "保存密码 "选项已经启用。我们将需要恢复这个密码。

事实上，有些网站不允许浏览器在自动完成的密码列表中保存密码。通常，这类网站是用JAVA编写的，或者它们使用其他的密码存储方法；例如，它们将密码存储在cookies中。

如果密码字段中充满了星号，解决办法很明确：选择ASTERISKS PASSWORDS操作模式，然后打开神奇的放大镜对话框。然后简单地将放大镜拖到Internet Explorer窗口（图6）

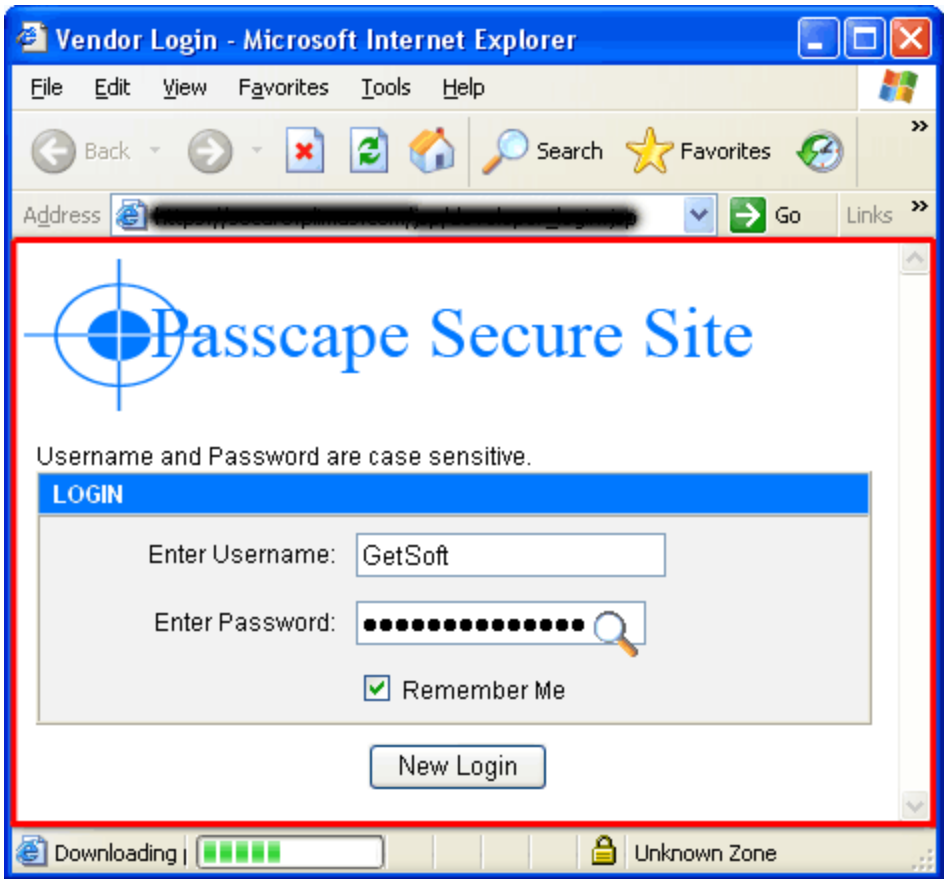

图6. 密码在星号的后面。

密码(密码，如果Internet Explorer窗口有几个带星号的字段)要出现在PIEPR窗口(图7)。

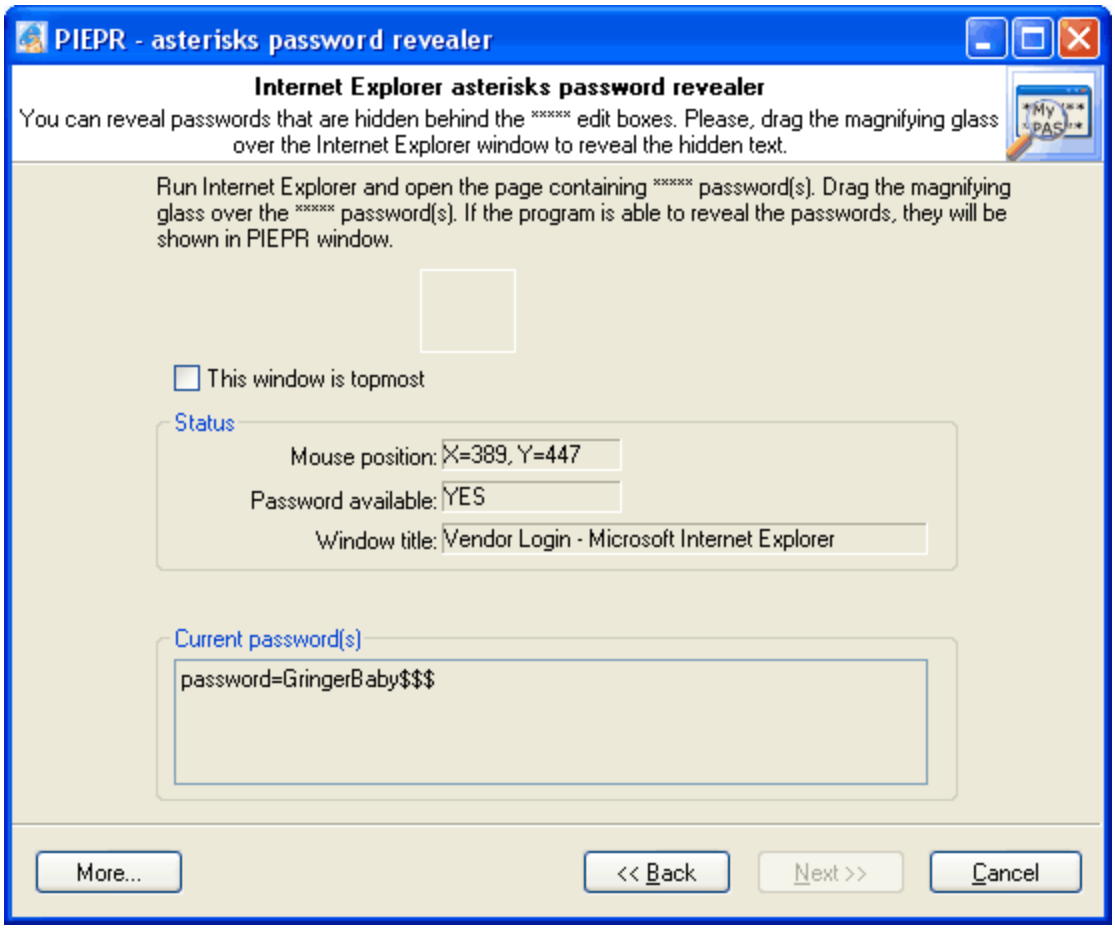

图7. 使用中的Magnifying glass。

但这并不总是那么简单。密码字段可能是空的，或者该字段可能确实包含*****。在这种情况下，正如你现在已经猜到的，ASTERISKS PASSWORDS工具将毫无用处。

我们可以假设，密码被储存在cookies中。让我们试着找到它。选择IE Cookie Explorer工具（图8）。

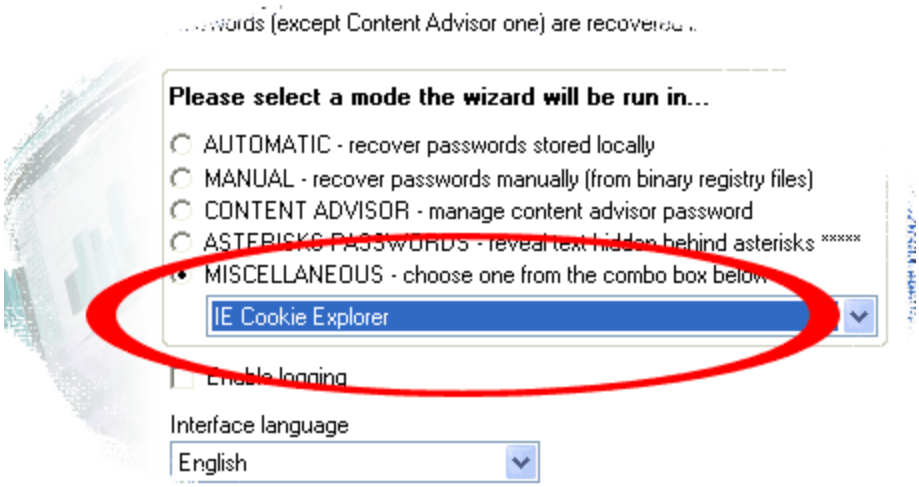

图8. IE Cookie Explorer。

出现的对话框将列出在您的计算机上存储cookie的网站。点击URL列的标题，按字母顺序排列网站列表。这将帮助我们更容易找到正确的网站。浏览网站列表，选择我们需要的网站。下面的列表将显示该网站的解密cookies（图9）。

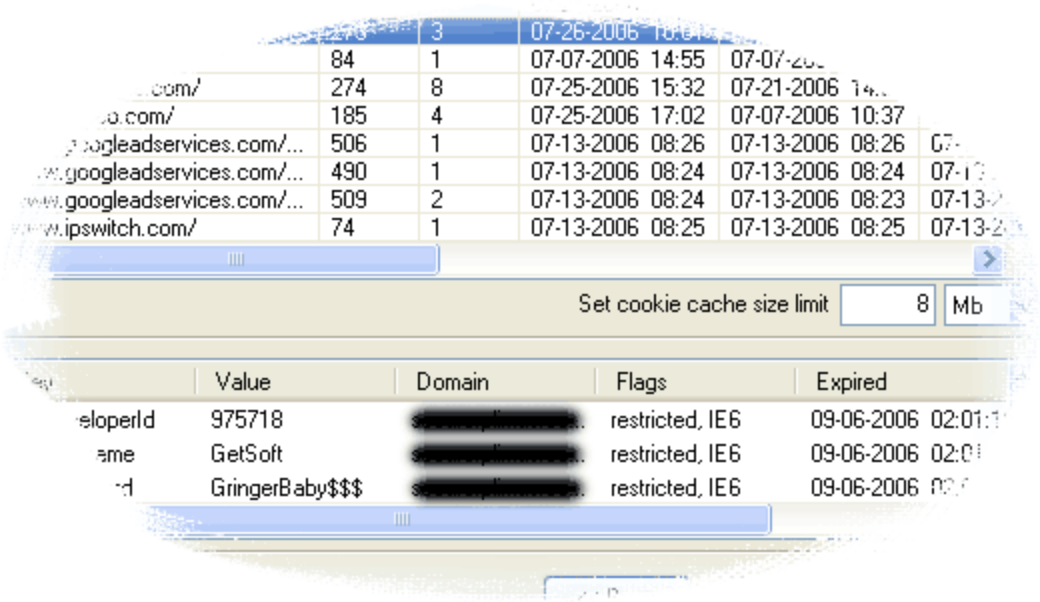

图9. 解密后的cookies。

如图所示，在我们的案例中，登录名和密码没有被加密，而是作为纯文本存储。

Cookies通常是加密的。在这种情况下，你不可能成功恢复密码。为了恢复旧账户，你唯一可以尝试做的事情是创建一个新账户。然后，你将能够在文本编辑器中复制旧的cookies，并用新的cookies替换它们。然而，这只是在最坏的情况下才有用，不建议正常使用。

不要忘记，几乎所有有密码的页面和表格都有 "忘记密码 "的按钮。

6 总结

正如本文所示，恢复Internet Explorer密码是一项非常简单的工作，不需要任何特殊的知识或技能。然而，尽管看起来很简单，但密码加密方案和算法都是经过深思熟虑的，而且实施得非常好。尽管 "保护存储 "的概念已有10多年的历史，但不要忘记，它已经证明了专家们的最佳建议，并且已经在这个流行的浏览器的三代中得到实施。

随着下一个，即第七个版本的IE的发布，微软正在准备从根本上保护我们的私人数据的新方案，它使用改进的加密算法并消除保护性存储特有的不足。

特别是，对Internet Explorer 7初步测试版本的分析表明，自动格式的密码加密密钥不再与数据一起存储。它们不再被存储，就这样 这是一个小技巧，专业人员和最终用户都要估计它的真正价值，无论如何，他们最终都会从中受益。

但最主要的是，新概念的发布将消除保护性存储所特有的主要缺点，即在不知道额外信息的情况下恢复密码的可能性。更好的说法是，这足以让潜在的黑客获得对硬盘内容的物理访问，以窃取或破坏密码和用户的其他私人数据。随着Internet Explorer 7的发布，情况会有一些改变。

与此同时，我们只能迫不及待地等待Windows Vista和IE 7的到来，以仔细观察这个流行的浏览器的下一代所使用的新加密机制