

مرسوم است و توصیه شده است که جهت ارائه کتابخانه‌های دات نت خود از امضای دیجیتال استفاده کنید. VS.NET برای این منظور در برگه signing خواص یک پروژه، چنین امکانی را به صورت توکار ارائه می‌دهد. حال اگر بخواهیم همین پروژه را به صورت سورس باز ارائه دهیم، استفاده کنندگان نهایی به مشکل برخورد؛ زیرا فایل pfx حاصل، توسط کلمه عبور محافظت می‌شود و در سایر سیستم‌ها بدون در نظر گرفتن این ملاحظات قابل استفاده نخواهد بود. معادل فایل‌های pfx، فایل‌هایی هستند با پسوند snk که تنها تفاوت مهم آن‌ها با فایل‌های pfx، عدم محافظت توسط کلمه عبور است و ... برای کارهای خصوصاً سورس باز انتخاب مناسبی به شمار می‌روند. اگر دقت کنید، اکثر پروژه‌های سورس باز دات نت موجود در وب (مانند NHibernate، لوسین، iTextSharp و غیره) از فایل‌های snk برای اضافه کردن امضای دیجیتال به کتابخانه نهایی تولیدی استفاده می‌کنند و نه فایل‌های pfx محافظت شده. در اینجا اگر فایل pfx ایی دارید و می‌خواهید معادل snk آن را تولید کنید، قطعه کد زیر چنین امکانی را مهیا می‌سازد:

```
using System.IO;
using System.Security.Cryptography;
using System.Security.Cryptography.X509Certificates;

namespace PfxToSnk
{
    class Program
    {
        /// <summary>
        /// Converts .pfx file to .snk file.
        /// </summary>
        /// <param name="pfxData">.pfx file data.</param>
        /// <param name="pfxPassword">.pfx file password.</param>
        /// <returns>.snk file data.</returns>
        public static byte[] Pfx2Snk(byte[] pfxData, string pfxPassword)
        {
            var cert = new X509Certificate2(pfxData, pfxPassword, X509KeyStorageFlags.Exportable);
            var privateKey = (RSACryptoServiceProvider)cert.PrivateKey;
            return privateKey.ExportCspBlob(true);
        }

        static void Main(string[] args)
        {
            var pfxFileData = File.ReadAllBytes(@"D:\Key.pfx");
            var snkFileData = Pfx2Snk(pfxFileData, "my-pass");
            File.WriteAllBytes(@"D:\Key.snk", snkFileData);
        }
    }
}
```

نظرات خوانندگان

نویسنده: Mohsen

تاریخ: ۱۱:۹ ۱۳۹۱/۰۷/۳۰

آقای نصیری ممنون از لطف شما. ممکنه بیشتر درمورد این امضا و نحوه‌ی کاربرد اون صحبت کنید؟(مثلا بنده یک کتابخانه‌ی آزمایشی را با استفاده از امضای موجود در بخش Signing امضا نموده و فایل pfx مربوطه را ساختم. اما اسمبلی مربوطه به سادگی در سایر پروژه‌ها قابل استفاده و حتی قابل مشاهده است(از طریق metadata)).

نویسنده: وحید نصیری

تاریخ: ۱۱:۱۲ ۱۳۹۱/۰۷/۳۰

بله. این امضای دیجیتال، فقط به این معنا است که کار تولید شده متعلق به شما می‌باشد. هیچ نوع محدودیت دیگری را اعمال نمی‌کند. + وجود آن اندکی patch کردن برنامه‌ها رو مشکل می‌کند. خصوصا در مورد برنامه‌های WPF و سیلورلایت.

نویسنده: سام ناصری

تاریخ: ۶:۲ ۱۳۹۱/۱۲/۱۶

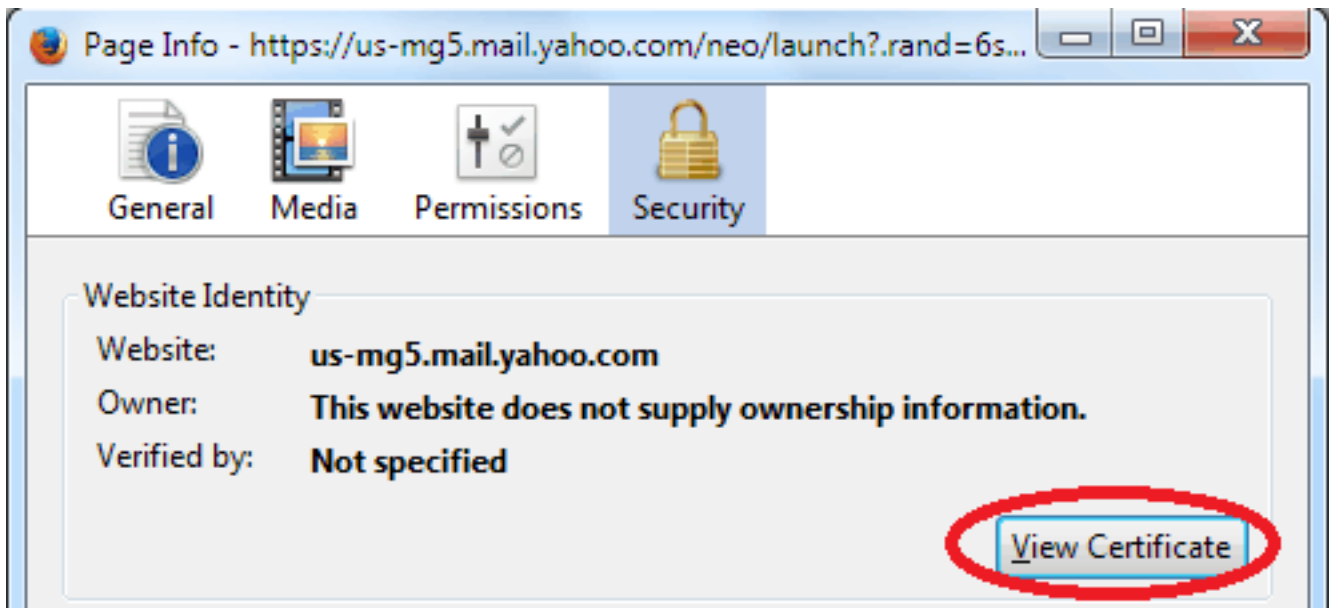
مطلب خوبی بود وحید جان. ممنونم. البته من بعد از اینکه مطلب شما رو خوندم و متوجه شدم که دو نوع فایل pfx و snk هست که با اون میشه sign کرد اندکی تو اینترنت گشتم و متوجه یک نکته شدم که گفتم بد نیست اینجا مطرح کنم. هر چند مطلب شما درباره تبدیل فایل pfx به snk است اما متنی که نوشتید این موضوع را القا میکند که نمیشود به سادگی این فایل رو ساخت. به هر روی، میتوان فایل snk را از طریق فایل زبانه signing در خواص پروژه ساخت. برای این کار کافیسست که گزینه Protect my key file with a password را آنتیک کرد و در این حالت به جای اینکه فایل pfx ساخته شود فایل snk ساخته میشود. مطلب دیگر اینکه من پروژه‌های متن باز دیگری را دیده ام که الان حضور ذهن ندارم بگم(احتمالاً یکیشون RavenDB بود) که از طریق خواص پروژه ویژوال استودیو کار signing را انجام نمیدهند یعنی در آنجا گزینه sign کردن را انتخاب نکرده اند. چون فایل snk را اگر منتشر کنیم همه میتونند با اون اسمبلی‌ها را sign کنند و معنای strong name بودن اسمبلی به طور کلی میره زیر سوال. در عوض از یک customized build استفاده میکنند که فقط توسط خودشون(مالکان پروژه) قابل فراخوانی است و توسط اون اسمبلی‌های release را میسازند. البته در اینباره باید بیشتر بررسی کنم و شاید دقیقاً ماجرا 100 درصد به این شکل که گفتم نیست.

نویسنده: وحید نصیری

تاریخ: ۹:۳۱ ۱۳۹۱/۱۲/۱۶

- علت اینکه این مطلب رو نوشتم مربوط به زمانی بود که پروژه‌ای از قبل موجود بود با فایل pfx آن و قصد داشتم معادل محافظت نشده فایل pfx آن را تولید کنم.
- در مورد تولید فایل‌های pfx و snk یک مطلب نسبتاً جامع [در سایت داریم](#) .
- به نظر من زمانیکه یک پروژه سورس باز است، امضا کردن اسمبلی‌های آن آنچنان مفهومی ندارد چون دسترسی به سورس و حتی ارائه آن بر اساس اطمینان به جامعه مصرف کننده صورت می‌گیرد. خیلی خیلی کم هستند موارد سوء استفاده از اسمبلی‌های امضاء شده به این صورت. مگر اینکه بحث پروژه کرنل لینوکس با تعداد مصرف کننده بالا و اهمیت امنیتی آن مطرح باشد که نیاز به امضای فایل‌های باینری آن وجود داشته باشد.

اگر به مرورگرها دقت کرده باشید، امکان نمایش SSL Server Certificate یک سایت استفاده کننده از پروتکل HTTPS را دارند. برای مثال در فایرفاکس اگر به خواص یک صفحه مراجعه کنیم، در برگه امنیت آن، امکان مشاهده جزئیات مجوز SSL سایت جاری فراهم است:



سؤال: چگونه می‌توان این مجوزها را با کدنویسی دریافت یا تعیین اعتبار کرد؟

قطعه کد زیر، نحوه دریافت مجوز SSL یک سایت را نمایش می‌دهد:

```
using System;
using System.Diagnostics;
using System.IO;
using System.Net;
using System.Security.Cryptography.X509Certificates;

namespace DownloadCerts
{
    class Program
    {
        static void Main(string[] args)
        {
            // صرفنظر از خطاهای احتمالی مجوز
            ServicePointManager.ServerCertificateValidationCallback = delegate { return true; };

            var url = "https://pdfreport.codeplex.com";
            var request = WebRequest.Create(url) as HttpWebRequest;
            request.Method = WebRequestMethods.Http.Head;
            using (var response = request.GetResponse())
            { /* در اینجا مجوز، در صورت وجود دریافت شده */ }






            if (request.ServicePoint.Certificate == null)
                return;

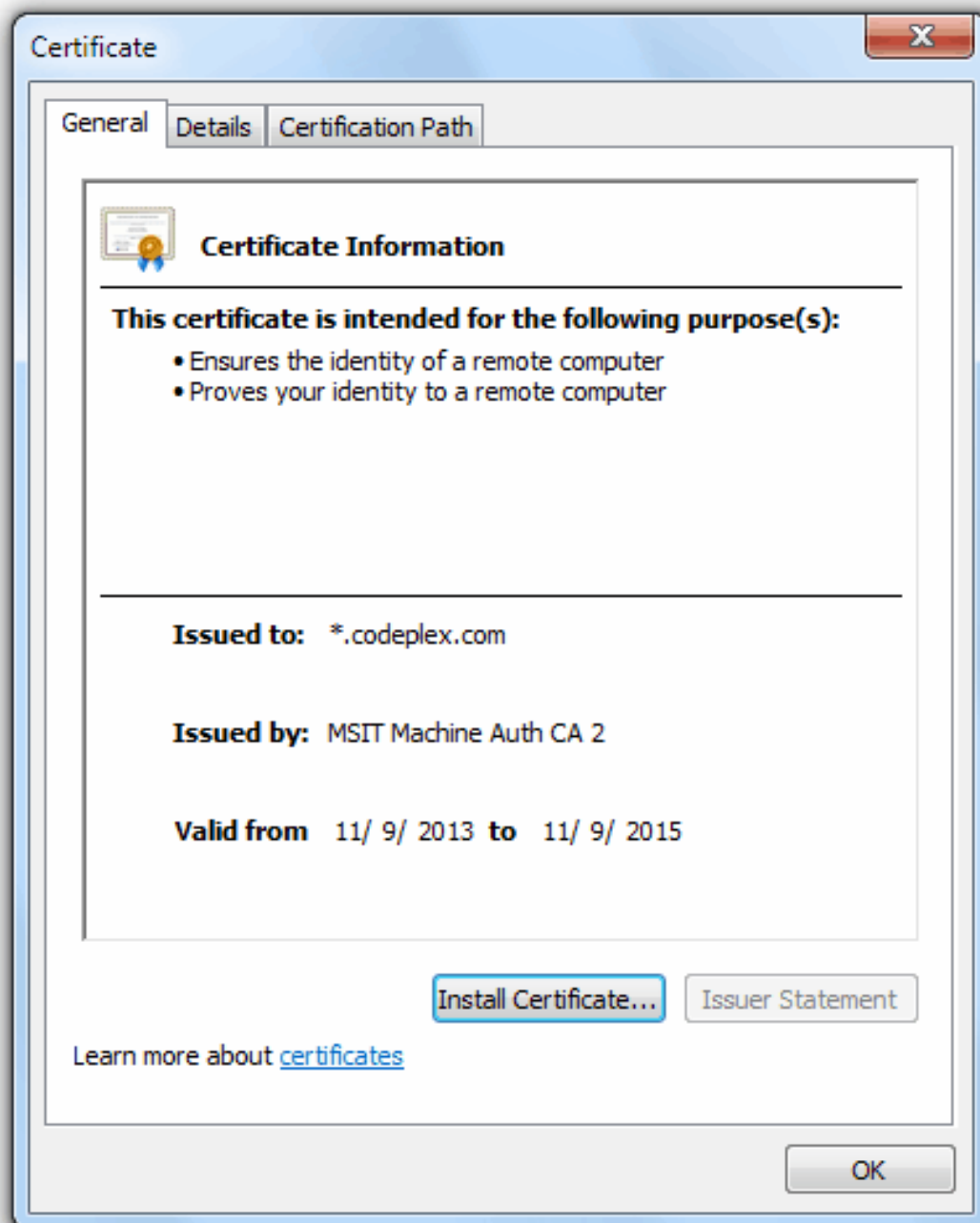
            // ذخیره سازی مجوز در فایل
            var cert = new X509Certificate2(request.ServicePoint.Certificate);
            Console.WriteLine("Expiration Date: {0}", cert.GetExpirationDateString());
            var data = cert.Export(X509ContentType.Cert);
        }
    }
}
```

```
        File.WriteAllBytes("site.cer", data);  
        Process.Start(Environment.CurrentDirectory);  
    }  
}
```

ممکن است مجوز یک سایت معتبر نباشد. کلاس `WebRequest` در حین مواجه شدن با یک چنین سایت‌هایی، یک `WebException` را صادر می‌کند. از این جهت که می‌خواهیم حتماً این مجوز را دریافت کنیم، بنابراین در ابتدای کار، `ServerCertificateValidation` را غیرفعال می‌کنیم.

سپس یک درخواست ساده را به آدرس سرور مورد نظر ارسال می‌کنیم. پس از پایان درخواست، خاصیت `request.ServicePoint.Certificate` با مجوز SSL یک سایت مقدار دهی شده است. در ادامه نحوه ذخیره سازی این مجوز را با فرمت `cer` مشاهده می‌کنید.

Name	Date modified	Type
 DownloadCerts.exe	۲۱ مهر ۱۳۹۲ ۱۲:۲۷ ق.ظ	Application
 DownloadCerts.pdb	۲۱ مهر ۱۳۹۲ ۱۲:۲۷ ق.ظ	PDB File
 DownloadCerts.vshost.exe	۲۱ مهر ۱۳۹۲ ۱۲:۲۹ ق.ظ	Application
 DownloadCerts.vshost.exe.manifest	۲۶ اسفند ۱۳۸۸ ۰۹:۳۹ ب.ظ	MANIFEST File
 site.cer	۲۱ مهر ۱۳۹۲ ۱۲:۲۹ ق.ظ	Security Certificate



نظرات خوانندگان

نویسنده: حمید حسین وند
تاریخ: ۱۶:۲۸ ۱۳۹۳/۰۱/۲۲

سلام؛ وقتی این گواهی یا certificate رو دانلود کردیم به چه دردمون میخوره؟ یعنی کاراییش برای ما چیه؟

نویسنده: وحید نصیری
تاریخ: ۱۶:۵۸ ۱۳۹۳/۰۱/۲۲

جهت بررسی اعتبار آن می‌تواند مفید باشد. مثلاً نوشتن برنامه‌ای مانند [SSL Certificate Verifier](#)

روش‌های زیادی برای ذخیره سازی کلمات عبور وجود دارند که اغلب آن‌ها نیز نادرست هستند. برای نمونه شاید ذخیره سازی کلمات عبور، به صورت رمزنگاری شده، ایده‌ی خوبی به نظر برسد؛ اما با دسترسی به این کلمات عبور، امکان رمزگشایی آن‌ها، توسط مهاجم وجود داشته و همین مساله می‌تواند امنیت افرادی را که در چندین سایت، از یک کلمه‌ی عبور استفاده می‌کنند، به خطر اندازد.

در این حالت هش کردن کلمات عبور ایده‌ی بهتر است. هش‌ها روش‌هایی یک طرفه هستند که با داشتن نتیجه‌ی نهایی آن‌ها، نمی‌توان به اصل کلمه‌ی عبور مورد استفاده دسترسی پیدا کرد. برای بهبود امنیت هش‌های تولیدی، می‌توان از مفهومی به نام Salt نیز استفاده نمود. Salt در اصل یک رشته‌ی تصادفی است که پیش از هش شدن نهایی کلمه‌ی عبور، به آن اضافه شده و سپس حاصل این جمع، هش خواهد شد. اهمیت این مساله در بالا بردن زمان یافتن کلمه‌ی عبور اصلی از روی هش نهایی است (توسط روش‌هایی مانند brute force یا امتحان کردن بازه‌ی وسیعی از عبارات قابل تصور).

اما واقعیت این است که حتی استفاده از یک Salt نیز نمی‌تواند امنیت بازایی کلمات عبور هش شده را تضمین کند. برای مثال نرم افزارهایی موجود هستند که با استفاده از پردازش موازی قادرند بیش از [60 میلیارد هش](#) را در یک ثانیه آزمایش کنند و البته این کارآیی، برای کار با هش‌های متداولی مانند MD5 و SHA1 بهینه سازی شده‌است.

روش هش کردن کلمات عبور در ASP.NET Identity

[ASP.NET Identity 2.x](#) که در حال حاضر آخرین نگارش تکامل یافته‌ی روش‌های امنیتی توصیه شده‌ی توسط مایکروسافت، برای برنامه‌های وب است، از استاندارد به نام RFC 2898 و الگوریتم PKDBF2 برای هش کردن کلمات عبور استفاده می‌کند. مهم‌ترین مزیت این روش خاص، کندتر شدن الگوریتم آن با بالا رفتن تعداد سعی‌های ممکن است؛ برخلاف الگوریتم‌هایی مانند MD5 یا SHA1 که اساساً برای رسیدن به نتیجه، در کمترین زمان ممکن طراحی شده‌اند.

PBKDF2 یا password-based key derivation function جزئی از استاندارد RSA نیز هست (PKCS #5 version 2.0). در این الگوریتم، تعداد بار تکرار، یک Salt و یک کلمه‌ی عبور تصادفی جهت بالا بردن انتروپی (بی‌نظمی) کلمه‌ی عبور اصلی، به آن اضافه می‌شوند. از تعداد بار تکرار برای تکرار الگوریتم هش کردن اطلاعات، به تعداد باری که مشخص شده‌است، استفاده می‌گردد. همین تکرار است که سبب کندشدن محاسبه‌ی هش می‌گردد. عدد معمولی که برای این حالت توصیه شده‌است، 50 هزار است. این استاندارد در دات نت توسط کلاس [Rfc2898DeriveBytes](#) پیاده سازی شده‌است که در ذیل مثالی را در مورد نحوه‌ی استفاده‌ی عمومی از آن، مشاهده می‌کنید:

```
using System;
using System.Diagnostics;
using System.Security.Cryptography;
using System.Text;

namespace IdentityHash
{
    public static class PBKDF2
    {
        public static byte[] GenerateSalt()
        {
            using (var randomNumberGenerator = new RNGCryptoServiceProvider())
            {
                var randomNumber = new byte[32];
                randomNumberGenerator.GetBytes(randomNumber);
                return randomNumber;
            }
        }

        public static byte[] HashPassword(byte[] toBeHashed, byte[] salt, int numberOfRounds)
        {
            using (var rfc2898 = new Rfc2898DeriveBytes(toBeHashed, salt, numberOfRounds))
            {
                return rfc2898.GetBytes(32);
            }
        }
    }
}
```

```

class Program
{
    static void Main(string[] args)
    {
        var passwordToHash = "VeryComplexPassword";
        hashPassword(passwordToHash, 50000);
        Console.ReadLine();
    }

    private static void hashPassword(string passwordToHash, int numberOfRounds)
    {
        var sw = new Stopwatch();
        sw.Start();
        var hashedPassword = PBKDF2.HashPassword(
            Encoding.UTF8.GetBytes(passwordToHash),
            PBKDF2.GenerateSalt(),
            numberOfRounds);

        sw.Stop();
        Console.WriteLine();
        Console.WriteLine("Password to hash : {0}", passwordToHash);
        Console.WriteLine("Hashed Password : {0}", Convert.ToBase64String(hashedPassword));
        Console.WriteLine("Iterations <{0}> Elapsed Time : {1}ms", numberOfRounds,
            sw.ElapsedMilliseconds);
    }
}

```

شیء Rfc2898DeriveBytes برای تشکیل، نیاز به کلمه‌ی عبوری که قرار است هش شود به صورت آرایه‌ای از بایت‌ها، یک Salt و یک عدد اتفاقی دارد. این Salt توسط شیء RNGCryptoServiceProvider ایجاد شده‌است و همچنین نیازی نیست تا به صورت مخفی نگهداری شود. آن‌را می‌توان در فیلدی مجزا، در کنار کلمه‌ی عبور اصلی ذخیره سازی کرد. نتیجه‌ی نهایی، توسط متد rfc2898.GetBytes دریافت می‌گردد. پارامتر 32 آن به معنای 256 بیت بودن اندازه‌ی هش تولیدی است. 32 حداقل مقداری است که بهتر است انتخاب شود.

پیش فرض‌های پیاده سازی Rfc2898DeriveBytes استفاده از الگوریتم SHA1 با 1000 بار تکرار است؛ چیزی که دقیقاً در ASP.NET Identity 2.x بکار رفته‌است.

تفاوت‌های الگوریتم‌های هش کردن اطلاعات در نگارش‌های مختلف ASP.NET Identity

اگر به [سورس نگارش سوم](#) ASP.NET Identity مراجعه کنیم، یک چنین کامنتی در ابتدای آن قابل مشاهده است:

```

/* =====
* HASHED PASSWORD FORMATS
* =====
*
* Version 2:
* PBKDF2 with HMAC-SHA1, 128-bit salt, 256-bit subkey, 1000 iterations.
* (See also: SDL crypto guidelines v5.1, Part III)
* Format: { 0x00, salt, subkey }
*
* Version 3:
* PBKDF2 with HMAC-SHA256, 128-bit salt, 256-bit subkey, 10000 iterations.
* Format: { 0x01, prf (UInt32), iter count (UInt32), salt length (UInt32), salt, subkey }
* (All UInt32s are stored big-endian.)
*/

```

در نگارش دوم آن از الگوریتم PBKDF2 با هزار بار تکرار و در نگارش سوم با 10 هزار بار تکرار، استفاده شده‌است. در این بین، الگوریتم پیش فرض HMAC-SHA1 نگارش‌های 2 نیز به HMAC-SHA256 در نگارش 3، تغییر کرده‌است.

در یک چنین حالتی بانک اطلاعاتی ASP.NET Identity 2.x شما با نگارش بعدی سازگار نخواهد بود و تمام کلمات عبور آن باید مجدداً ریست شده و مطابق فرمت جدید هش شوند. بنابراین امکان انتخاب الگوریتم هش کردن را نیز [پیش بینی کرده‌اند](#).

در نگارش دوم ASP.NET Identity، متد هش کردن یک کلمه‌ی عبور، چنین شکلی را دارد:

```

public static string HashPassword(string password, int numberOfRounds = 1000)
{

```



```
if (password == null)
    throw new ArgumentNullException("password");

byte[] saltBytes;
byte[] hashedPasswordBytes;
using (var rfc2898DeriveBytes = new Rfc2898DeriveBytes(password, 16, numberOfRounds))
{
    saltBytes = rfc2898DeriveBytes.Salt;
    hashedPasswordBytes = rfc2898DeriveBytes.GetBytes(32);
}
var outArray = new byte[49];
Buffer.BlockCopy(saltBytes, 0, outArray, 1, 16);
Buffer.BlockCopy(hashedPasswordBytes, 0, outArray, 17, 32);
return Convert.ToBase64String(outArray);
}
```

تفاوت این روش با مثال ابتدای بحث، مشخص کردن طول salt در متد [Rfc2898DeriveBytes](#) است؛ بجای محاسبه‌ی اولیه‌ی آن. در این حالت متد Rfc2898DeriveBytes مقدار salt را به صورت خودکار محاسبه می‌کند. این salt بجای ذخیره شدن در یک فیلد جداگانه، به ابتدای مقدار هش شده اضافه گردیده و به صورت یک رشته‌ی base64 ذخیره می‌شود. [در نگارش سوم](#)، از کلاس ویژه‌ی RandomNumberGenerator برای محاسبه‌ی Salt استفاده شده‌است.

نظرات خوانندگان

نویسنده: امیر صیدی لو
تاریخ: ۱۳۹۴/۰۴/۱۵ ۶:۳۴

ممنون از مطلب خوبتون
ولی یه مشکلی که من موقع تست برخورددم این بود که زمان تبدیل آرایه تولید شده به وسیله تابع HashPassword به معادل رشته ای اون برای ذخیره در دیتابیس و بازیابی اون رشته به معادل آرایه اون برای چک کردن صحت کلمه عبور هر دو مقدار قبل از تبدیل و بعد از تبدیل با هم برابر بودن و مشکلی نداشتن ولی هنگام همین عمل تبدیل برای مقدار salt و بازیابیش از دیتا بیس مقدار قبل تبدیل و بعدش یکسان نبودن به همین خاطر مجبور شدم مقدار salt رو به صورت آرایه توی دیتابیس ذخیره کنم، خروجی حاصل از salt هم چک کردم نمی‌دونم چرا آرایه حاصل بیشتر از 32 خانه بود؟

نویسنده: وحید نصیری
تاریخ: ۱۳۹۴/۰۴/۱۵ ۱۰:۴

در ASP.NET Identity جمع هش و salt با فرمت base64 در بانک اطلاعاتی به صورت رشته‌ای با طول max ذخیره می‌شوند (هر دو با هم در یک فیلد). همچنین در اینجا طول salt به صورت صریح به 16 بایت تنظیم شده‌است (متد آخر مطلب).

Id	AddressId	Email	EmailConfirmed	PasswordHash
1	4	admin@example.com	0	ANMiCgyPWK3b94BFuJARK5+7
2	5	test@site.com	1	ACmZA5Fqgv1+2uALK5UpGrZ0HE

نویسنده: امیر صیدی لو
تاریخ: ۱۳۹۴/۰۴/۱۵ ۱۰:۳۵

تو این حالت (یکی کردن salt و hashPassword) چطوری می‌تونیم مقدار salt رو از دیتا بیس بخونیم و با کلمه عبور ورودی کاربر جمع بزنیم و با مقدار hashPassword اولیه مقایسه کنیم؟

نویسنده: وحید نصیری
تاریخ: ۱۳۹۴/۰۴/۱۵ ۱۱:۹

از متدهای HashPassword و VerifyHashedPassword [سورس ASP.NET Identity](#) ایده بگیرید. مورد اول برای ذخیره سازی اطلاعات در بانک اطلاعاتی است. مورد دوم در حین لاگین، جهت تعیین اعتبار کلمه‌ی عبور کاربر استفاده می‌شود.

یکی از روش‌های ارسال و رمزگذاری اطلاعات، استفاده از کلیدهای امنیتی مورد استفاده‌ی در سیستم یونیکس یا [GnuPG](#) است. استفاده از نرم افزار Gnu Privacy Guard یا گارد حفاظتی گنو، به ما این اجازه را می‌دهد که بتوانیم اطلاعاتمان را در بسترهای ارتباطی، با خیالی راحت‌تر ارسال کنیم و تا حد زیادی مطمئن باشیم که تنها فرد هدف توانایی دسترسی به اطلاعات را خواهد داشت. گارد امنیتی گنو زیر مجموعه‌ای از پروژه‌ی گنو است که دولت آلمان پایه ریز اصلی آن بوده است. این نرم افزار از یک روش رمزگذاری ترکیبی استفاده می‌کند که الگوریتم‌های [کلیدهای برابر\(مقارن\)](#) و [کلیدهای عمومی \(نامقارن\)](#) جهت تبادل آسان کلید را شامل می‌شود. در حال حاضر که نسخه‌ی دو این برنامه ارائه شده است، برای رمزگذاری‌ها از کتابخانه‌ای به اسم [libgcrypt](#) استفاده می‌کند. یکی از مشکلات فعلی این پروژه، عدم وجود api مناسبی جهت دسترسی راحت‌تر است و برای حل این مشکل، GPGME که مخفف GnuPG Made Easy ایجاد شد. بسیاری از برنامه‌ها و پلاگین‌های ارسال اطلاعات، امروزه همچون ارسال ایمیل، از این کلیدها بهره می‌برند.

پروژه‌های مرتبط با این قضیه اسم‌های مشابهی دارند که گاهی بعضی افراد، هر کدام از اسم‌ها را که دوست دارند، به همه اطلاق می‌کنند؛ ولی تفاوت‌هایی در این بین وجود دارد:

OpenPGP: یک برنامه نیست و یک قانون و استاندارد برای تهیه‌ی آن است؛ که رعایت اصول آن الزامی است و برنامه‌ی بالا، یک پیاده سازی از این استاندارد است.

PGP: یک برنامه، برای رمزگذاری اطلاعات است که مخفف [Pretty Good Privacy](#) است.

و **GnuPG** یا **GPG** که در بالا به آن اشاره شد.

برای ساخت کلید، ما از دستور یا برنامه‌ی GPG که که عمدتاً در همه‌ی لینوکس‌ها مثل دبیان و مشتقات آن نصب است، استفاده می‌کنیم و اگر نصب نیست از طریق توزیع آن اقدام نمایید.

در صورتیکه از ویندوز استفاده می‌کنید، نیاز است ابتدا خط فرمان یونیکس را روی آن نصب کنید. برنامه‌ی [Cygwin](#) این امکان را به شما می‌دهد تا خط فرمان یونیکس و دستورات پیش فرض آن را داشته باشید. این برنامه در دو حالت ۳۲ بیتی و ۶۴ بیتی ایجاد شده است. از آنجا که گفتیم این برنامه شامل دستورات پیش فرض آن است، برای همین GPG باید به صورت یک بسته‌ی جداگانه نصب شود که در [سایت آن](#) می‌توانید بسته‌های مختلف آن را برای پلتفرم‌های مختلف را مشاهده کنید.

ساخت کلید

برای ساخت کلید دستور زیر را صادر کنید:

```
gpg --gen-key
```

اگر از نسخه‌های جدیدتر GPG استفاده می‌کنید، گزینه‌هایی به شکل زیر ایجاد می‌شوند؛ ولی اگر خیر، ممکن است تعداد و شمارهی گزینه‌ها متفاوت باشند که در این مورد دقت کنید. من در اینجا همان حالت پیش فرض، یعنی ۱ را انتخاب می‌کنم. این گزینه نحوه‌ی امضاء و یا رمزگذاری شما با استفاده از الگوریتم‌های [RSA](#) و [DSA](#) را مشخص می‌کند.

Please select what kind of key you want:

- (1) RSA and RSA (default)
- (2) DSA and Elgamal
- (3) DSA (sign only)
- (4) RSA (sign only)

در کل در هر حالتی، استفاده‌ی از RSA پیشنهاد می‌شود. بعد از آن، از شما اندازه‌ی کلید را می‌پرسد که همان مقدار پیش فرض خودش را وارد می‌کنیم:

What keysize do you want? (2048)

البته بسیاری ۲۰۴۸ بیت را نیز کافی می‌دانند.
بعد از آن مدت زمان اعتبار این کلید را از شما جویا می‌شود:

Key is valid for? (0)

هنگام این پرسش نحوه‌ی ورود زمان را به شما خواهد گفت که می‌تواند به شکل‌های زیر باشد:

دو هفته
2w
دو سال
2y

پس از آن هم یک تاییدیه از شما می‌گیرد و تاریخ انقضاء را به طور کامل برای شما می‌نویسد و سپس نیاز است که اطلاعاتی از قبیل نام و ایمیل و توضیح را وارد کنید:

You need a user ID to identify your key; the software constructs the user ID from the Real Name, Comment and Email Address in this form:
"Heinrich Heine (Der Dichter) <heinrich@duesseldorf.de>"

Real name: ali yeganeh.m
Email address: yeganehaym@gmail.com
Comment: androidbreadcrumb
You selected this USER-ID:
"ali yeganeh.m (androidbreadcrumb) <yeganehaym@gmail.com>"

بعد از آن از شما می‌خواهد که کل عملیات را تایید و یا کنسل کنید؛ یا اگر اطلاعات بالا را اشتباه وارد کرده‌اید، اصلاح کنید. با زدن کلید 0 عملیات را تایید کنید. در این حین از شما یک کلید برای رمزگذاری می‌پرسد که باید آن را دو بار بدهید و کارتان در اینجا به پایان می‌رسد و کلید ایجاد می‌شود.
اگر مشکلی در ساخت کلید نباشد با ارسال دستور زیر باید آن را در لیست کلیدها ببینید:

```
ali@alipc:~$ gpg --list-keys
/home/ali/.gnupg/pubring.gpg
-----
pub 2048R/8708016A 2015-10-23 [expires: 2065-10-10]
uid ali yeganeh.m (androidbreadcrumb) <yeganehaym@gmail.com>
sub 2048R/533B7E96 2015-10-23 [expires: 2065-10-10]
```

در اینجا کلید عمومی در خط pub بعد از / قرار دارد؛ یعنی عبارت ۸۷۰۸۰۱۶A کلید عمومی ماست که بر روی هر سیستم و هر کلیدی متفاوت است.

تبدیل کد متنی به کد دودویی

یکی از روش‌های ارسال کدهای دودویی تبدیل آنان به یک قالب متنی ASCII است که به آن قالب [ASCII Armor](#) هم می‌گویند. سایت‌های زیادی وجود دارند که این عبارت متنی را از شما می‌خواهند. چرا که مثلاً این امکان وجود دارد که کلیدی که کاربر به سمت آنان می‌فرستد، آسیب دیده باشد یا اینکه KeyServerها در دسترس نباشند. در مورد این سرورها در ادامه صحبت خواهیم کرد. مثلاً یکی از سایت‌هایی که به این عبارت‌ها نیاز دارد [Bintray](#) است.

برای دریافت این کلید متنی باید دستور زیر را صادر کنید:

```
gpg --output mykey.asc --export -a $GPGKEY
```

که برای مثال ما می‌شود:

```
gpg --output mykey.asc --export -a 8708016A
```

و اگر کلید را با یک ویرایشگر متنی باز کنید، محتوایی شبیه محتوای زیر را خواهید دید:

```
ali@alipc:~$ cat mykey.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQENBFYqAJABCAdcw5xPonh5Vj7nDk1CxDskq/Vs008X0a/i20L0zatB4oK5x+0x
jxORxMnIAR83PCK5/Wk0Ba64jnu3eiP3jKEwAyKGGZ/Z1bezC9TIP8y+PnsiDhT
aFarluUJx+RT5q7s27aKjqoc3fR/xuwlWopZt9uYzE/DQAPDsHdUoUg+fh4Hevm+
a8/3ncR7q6nM8gc9wk621Urb1HaRrILdmeh7ZpJc18ZUbc+N0bw357fGsJnpfHX0
rdCr7C1vNUq6I+IeGMQG/6040LeeaqhaRxPrUhbFjLA155gkSqzecx17wQaYc71M
Zdlv+6Pt1B8nPAA3WxQ0ypjU8A5bvmAQRD5LABEBAAG0GFsaSB5ZWdhbmVoLm0g
KGFuZHZJvawRicmVhZGNYdW1kSA8eWVnYw5laGF5bUBnbWfPpbC5jb20+iQE+BBMB
AgAoBQJWkgCQAhsDBQ1d/A8ABgsJCAcDAgYVCAIJCgsEFgIDAQIeAQIXgAAKCRDS
Lhq8hwgBanaHB/4reGxUjR6dB08ykfwQOx+raYHGqJ1lgawisE4qUHTkGaspyQaNy
yxh0vWkKvg6nNy2VN1XFbc7j1H1rYqPPuPdG2B+1LvEghb30ESDbHUvk8NrJgDJ
C0257gxqWvUQTWvMC3FkSLdw3tyQ8dF7FxmSU79XcxVqGeseaDzMQrEasP0yJHsm
NJf8pvuD6qiWu3KSSoQmI/17Sj8s7eGJMh6o5YRFgHc1Bt9tCD+52bvt579Ju4vZ
tmQvXR4fNQo9sAeMqAJhIpF7IYcuyCEy+CQ847UkzE4f/OCCPxfV3samV/nnBJJ9
Ouu+681k6Fpx4A0a3nEwqoAmMwXrbSSUFW97uQENBFYqAJABCAC4CzrUOKskE4hK
GVCja0JKxhbuUdOrep6n3vof0fscs5Dy7h2oVh2vb12WH9X6pijJVPiUpGR4Mpu0
102Bu9Rwt38AQ6mRmL/hfzjEXSvKkdX7osk+1CVnnUaSDm9Ek2hWUH8JcN28z/WT
X9Bw8MCDZF7j1HvX/5ojghzMZYm4e1WJLBr1gON6xXAI6HR7D1nRkaVr8L9SYGm
FyAXZ0LzWYwG1Z1AntYxf6v/Mn3p1/1E3aBA+LkQqBzHg2nBm4jCaFwFeCdINBf
CHkY9r/Evo9hUPD+CtBNFwsUm1D4maz0FFtIQ701QhVmupnub+rKo0bC0AFj3abK
MCw9uo8TABEBAAGJASUEGAECaA8FAlYqAJACGwwFCV38DwAACgkQ0i4avIcIAWrz
rAf+K1IIMtBq3WlabfZQrgzFHQ62ugVJO/yI1ITkm4l08XHDf+ShqDg4urNumDEe
oQD35MvB2BhER1jL6VR3qjLkZyZYJ+EQiSxEDWxooav3KvpWjhcqjQy79GFs8waH
E7ssGmWwaugVS/PJAmGQ+s8YWDNa6aCC1mp2dJRiwbTyFdeWNBLa2V32xzWCYxhI
YtEp+K15XuCDTRatOPWFSFGSPe/paytmpGZc0XzU/W9sBpabhxVmcL4H6L07uCeF
IOOn/S5QXo3P9X/3ckmJ9GUb7rjdq1ivYgX53xI75jlePsmN/2f+3fNffUaZgFTTd
Uls+XCun70VYSBBfjgRfQbTvoA==
=6j7i
-----END PGP PUBLIC KEY BLOCK-----
```

در صورتی که قصد دارید متن کلید خصوصی را به دست بیاورید، لازم است بعد از export- عبارت secret-key- را نیز اضافه کنی
د؛ یعنی:

```
gpg --output mykey.asc --export-secret-key -a 8708016A
```

آپلود کلید به سرورهای کلید (Key Servers)

یکی از روش‌های به اشتراک گذاری کلید برای کاربران این است که از [سرورهای کلید](#) استفاده کنیم. یکبار آپلود روی یکی از این سرورها باعث می‌شود که به بقیه‌ی سرورها هم اضافه شود. یکی از این سرورهای کلید که خودم از آن استفاده می‌کنم، سرور ابونتو است و با استفاده از دستور زیر، همان کلید بالا را برای آن سرور ارسال می‌کنم:

```
gpg --send-keys --keyserver keyserver.ubuntu.com $GPGKEY
==>
gpg --send-keys --keyserver keyserver.ubuntu.com 8708016A
```

سپس از طریق کلید متنی، کلید آپلود شده را تایید می‌کنیم. به [این آدرس](#) رفته و محتوای کلید متنی خود را به طور کامل به همراه تگ‌های شروع و پایان کپی کنید و حتی می‌توانید کلید خود را از طریق کادر جست و جو پیدا کنید.

رمزگذاری

ابتدا در محیط یونیکس، یک فایل متنی ساده با متن hello ubuntu را ایجاد می‌کنم. در ادامه قصد دارم این فایل را رمزنگاری کنم:

```
ali@alipc:~$ cat >ali.txt
hello ubuntu
```

سپس همین فایل را رمزنگاری می‌کنم:

```
ali@alipc:~$ gpg --output myali.gpg --encrypt --recipient yeganehaym@gmail.com ali.txt
```

در این دستور ابتدا گفتیم که نام فایل خروجی ما myali.gpg است و می‌خواهیم آن را رمزگذاری کنیم که توسط کلیدی با ایمیل yeganehaym@gmail.com می‌باشد فایل ali.txt را رمزگذاری می‌کنیم.

رمزگشایی

برای رمزگشایی می‌توانید از طریق دستور زیر اقدام کنید:

```
gpg --output output.txt --decrypt myali.gpg
```

```
You need a passphrase to unlock the secret key for
user: "ali yeganeh.m (androidbreadcrumb) <yeganehaym@gmail.com>"
2048-bit RSA key, ID 533B7E96, created 2015-10-23 (main key ID 8708016A)
```

در اینجا دستور دادیم محتوای فایل رمزشده‌ی myali.gpg را رمزگشایی کن و محتوای آن را داخل فایلی با نام output.txt قرار بده. بعد از اجرای این دستور از شما عبارت رمزی را که در مرحله‌ی ساخت کلید دوبار از شما پرسید، درخواست می‌کند. در بعضی سیستم‌ها در همان ترمینال می‌پرسد، ولی بعضی سیستم‌ها مثل ابونتو که من از آن استفاده می‌کنم، به صورت گرافیکی یک کادر باز کرده و از شما خواهش می‌کند عبارت رمز را وارد کنید. عبارت رمز را وارد کنید و حالا فایل output.txt را باز کنید:

```
ali@alipc:~$ cat output.txt
hello ubuntu
```