مبانی امنیت شبکه

پاسخ سوالات پروژه 2

علی مهرانی - 810198542

پاسخ سوالات بخش 1

- تفاوت فایل های pfx، cer و pem در چیست؟

توضیحاتی درباره هرکدام و تفاوت هایشان ارائه می دهیم.

فایل pfx فرمت خاصی است که برای ذخیره سازی کلید عمومی و کلید خصوصی و certificate مربوطه یا همان گواهی دیجیتال استفاده می‌شود. عمدتا از این فایل برای موارد مربوط به tls/ssl مثلا برای یک وبسایت یا برای موارد امنیتی مربوط به ایمیل، برای امضای دیجیتال استفاده می شود. این فایل به جهت تامین امنیت، معمولا با یک رمز عبور محافظت می‌شود. فایل pfx دارای پسوند pfx یا p12 می باشد.  این فایل نباید خارج از سازمانی که از آن استفاده می کند، به اشتراک گذاشته شود.

فایل cer فرمت خاصی است که تنها شامل کلید عمومی و اطلاعات شناسایی دیگر است. در فرآیند ssl handshake این فایل از سوی سرور به کلاینت ارسال می شود و میتوان محتوای آن را در مرورگر بررسی کرد. از cer برای اشتراک گذاری public key نیز استفاده می شود.

فایل pem یا privacy enhanced mail یک فرمت استاندارد برای ذخیره سازی انواع داده های cryptographic از جمله certificate ها و. کلید های خصوصی که این دو مورد می توانند در فایل‌های جدا یا در کنار هم باشند. این فایل در تنظیمات apache server و nginx استفاده می‌شود.

**تفاوت ها:** cer برخلاف pfx تنها دارای کلید عمومی است و شامل کلید خصوصی نیست. فایل pfx بر خلاف دو فایل دیگر، با رمز عبور محافظت می‌شود و فایل pem از رمزنگاری base64 استفاده می‌کند. فایل cer بیشتر برای اشتراک‌گذاری کلید عمومی استفاده می‌شود. فایل pem می‌تواند شامل کلید خصوصی باشد اما cer خیر.

- چرا روی فایل pfx پسورد گذاشته می شود؟ این پسورد چه نقشی در کلید های عمومی و خصوصی دارد؟

دلیل آن به طور کلی این است که فایل pfx مقدار private key را با آن password رمز میکند تا اگر فایل به دست کسی افتاد، محتویات کلید خصوصی نمایان و visible نباشد و فقط برای کسی که password را دارد، مشخص باشد. با این کار امکان استفاده از کلید خصوصی توسط یک شخص unauthorized وجود نداشته باشد.
برای فرستادن یک ایمیل امن به این certificate نیاز داریم و سیستم سرویس ایمیل که در این جا outlook است، باید به کلید خصوصی دسترسی داشته باشد تا بتواند چیزی را امضا کند و نقش password نیز رمزنگاری و محافظت از این کلید خصوصی است. کلید عمومی از طرفی رمز نشده و قابل رویت است و در صورتی که پیامی با کلید خصوصی فرستنده رمزنگاری شود، تنها با کلید عمومی آن فرستنده رمزگشایی می شود و از این در فرآیند امضا دیجیتال استفاده می شود. در فایل pfx مقدار کلید عمومی قابل رویت است و رمز نشده.

- چرا برای انجام این تمرین نیاز به یک کلاینت ایمیل مانند Microsoft Outlook داریم؟

به این دلیل که web application های سرویس‌دهنده ایمیل مانند gmail از S/MIME پشتیبانی نمی‌کنند و تنها کلاینت‌های خاصی مانند outlook از آن پشتیبانی می‌کنند و به این جهت، در صورتی که بخواهیم به قابلیت‌هایی از جمله ارسال و دریافت ایمیل رمز شده و امضا کردن ایمیل و یا بررسی امضا ایمیل دریافتی، دسترسی داشته باشیم، باید از کلاینتی مانند outlook استفاده کنیم که از S/MIME پشتیبانی کند.

- در صورتی که یک ایمیل به همین صورت امضا شده و رمز شده را به یک فرد بدون کالینت ایمیل بفرستید (مثلا یک ایمیل Gmail که از طریق وب اپلیکیشن مرورگر استفاده می گردد)، امضای دیجیتال و رمزنگاری در سمت گیرنده چگونه بروز می یابد؟ (پیشنهاد می شود این کار را انجام دهید).

جیمیل یا کلاینت‌های دیگری که S/MIME را پشتیبانی نمی‌کنند، قابلیت انتخاب کلید عمومی یا خصوصی را ندارند و به این دلیل چون کلید عمومی ثبت نشده است، امکان رمزنگاری پیام وجود ندارد. بنابراین نمی‌شود از outlook پیامی را برای گیرنده (کلایتنی) که از S/MIME پشتیبانی نمی‌کند، رمز کرد. این مسئله همچنین برای امضا کردن نیز وجود دارد و اگر گیرنده از S/MIME پشتیبانی نکند، اگر پیام امضا شده ای دریافت کند، آن را ignore میکند چون که آن را نمی‌شناسد و ایمیل نمایش‌داده شده به کاربر درواقع به گونه‌ای است که انگار اصلا از اول امضا نشده است.