فناوری‌های محافظت کننده

همه چیزی که باید درباره رمزنگاری ایمیل بدانید!

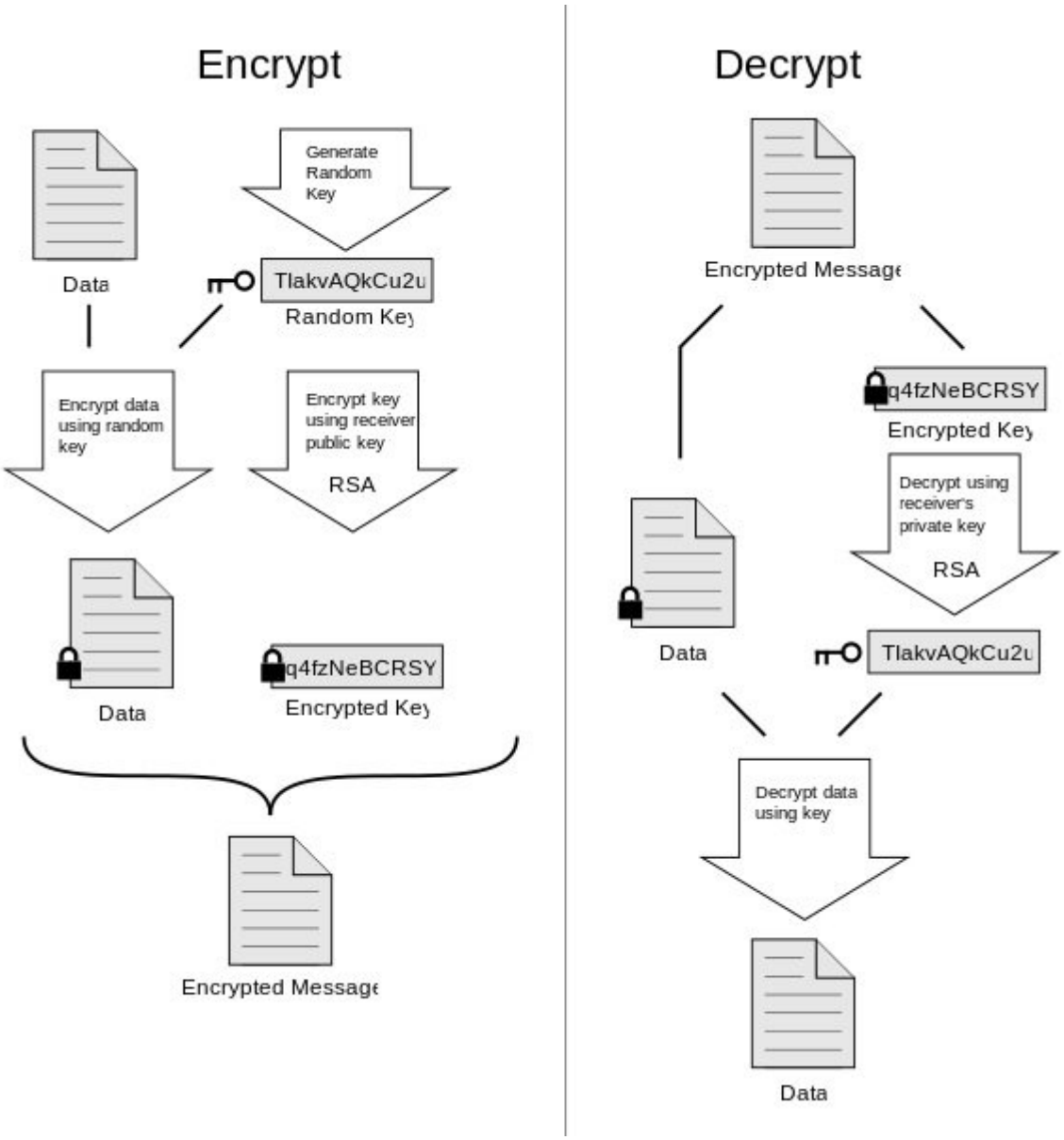
محافظت از پست‌الکترونیک به معنای حفاظت از حریم خصوصی است. عدم توجه به اصول ساده اما زیربنایی باعث می‌شود که نه تنها ایمیل‌ها به آسانی مورد سوءاستفاده قرار گیرند، بلکه احتمال دسترسی‌های غیرمجاز به یک سیستم که از طریق یک ضمیمه آلوده ارسال شده است را ساده می‌کند. رمزنگاری ایمیل‌ها یکی از ساده‌ترین و مؤثرین روش‌های محافظت از محتوای دیجیتالی است.

جای تعجب است که چرا هنوز هم خیلی از مردم درباره امن‌سازی پست‌الکترونیک خود اطلاعی ندارند. البته امروزه سطح آگاهی مردم خیلی بیشتر از گذشته شده است و مردم درباره وجود هرزنامه‌ها اطلاع کافی دارند. اما خیلی از مردم داستان‌های ترسناکی از ارسال اشتباهی یک ایمیل یا عدم بررسی آدرس ایمیل گیرنده در کادر مربوطه، زمانی که روی دکمه Reply All کلیک کرده‌اند، در ذهن دارند. اما آن‌ها از وجود مسائل اساسی و زیربنایی که به راحتی می‌تواند حریم خصوصی آن‌ها را در معرض خطر قرار دهد، اطلاعی ندارند.

زمانی‌که نزدیک به چهل سال پیش پست‌الکترونیک اختراع شد، هیچ کس از این‌که چگونه می‌تواند یک ایمیل یکپارچه را ارسال کند ذهنیتی نداشت. در نتیجه، ارسال ایمیل‌های جعلی برای هر شخصی به راحتی امکان‌پذیر بود، اما اطمینان از این‌که ایمیل ارسال شده از طرف همان شخصی است که باید آن‌را ارسال می‌کرده است کار بسیار مشکلی بود. به دلیل این‌که یک متن خام روی بستر اینترنت ارسال می‌شد، در نتیجه هیچ ویژگی یا به عبارت دقیق‌تر اصل محرمانگی روی محتوای ایمیل وجود نداشت، به طوری که ارسال یک کارت پستال امنیت بیشتری نسبت به یک ایمیل داشت. حتی برنامه‌های پیام‌سان فوری نیز امنیت بیشتری نسبت به پست‌الکترونیک دارند. اما برای همه مردم نگرانی از بابت حفظ حریم خصوصی وجود دارد. بیشتر مردم از این‌که پیام‌های ایمیل آن‌ها توسط هر شخصی قابل خواندن است، اطلاعی ندارند. رمزنگاری کلید حل این مشکلات است. اما زمانی‌که کاربر از این فناوری استفاده کند و موارد مربوط به آن‌را فراموش کند، تبدیل به یک چالش بزرگ می‌شود. رمزنگاری به طور ناخودآگاه و به شیوه معجزه‌آسا اجرا نمی‌شود. به‌کارگیری این فناوری نیاز به کمی تلاش دارد. ما در این مقاله به بررسی سه گزینه مختلف که برای رمزنگاری وجود دارد، می‌پردازیم و همچنین به نقاط قوت و ضعف این سه فناوری اشاره‌ای خواهیم کرد. اما به عنوان یک اصل کلی، بخش بزرگی از کار به یادگیری مسائل امنیتی توسط کاربران باز می‌گردد، پس سعی کنید زمانی‌که از این روش‌ها استفاده می‌کنید اطلاعات اولیه را پیرامون امنیت به دست آورید.

PGP و S/MIME

PGP سرنام (Pretty Good Privacy) و S/MIME (سرنام Secure/Multipurpose Internet Mail Extensions) از رایج‌ترین استانداردها برای رمزنگاری و ورود به ایمیل هستند. در حالی‌که پی‌جی‌پی به آسانی قابل راه‌اندازی است، اما زیاد کاربرپسند نبوده و به خوبی با برنامه‌های ایمیل همچون آوت‌لوک ادغام نمی‌شود. این نرم‌افزار که برای رمزگذاری و رمزگشایی مورد استفاده قرار می‌گیرد، برای اطمینان از هویت گیرنده و فرستنده داده‌ها در زمان جابه‌جایی و تبادل داده‌ها و کنترل حفظ حریم خصوصی مورد استفاده قرار خواهد گرفت. تصویر زیر فرآیند رمزنگاری و رمزگشایی در PGP را نشان می‌دهد.



توسعه چندمنظوره پست الکترونیک امن S/MIME که بر مبنای رمزنگاری با کلیدعمومی و امضا برای MIME کار می‌کند، از یک سازمان‌دهی دوستانه‌تری برخوردار بوده و به آسانی قابل راه‌اندازی است. اما برای این‌که بتواند به خوبی کار کند، هر کاربر نیاز به یک گواهی تصدیق هویت عمومی که از مراکز صدور گواهی (CA)به دست می‌آید، نیاز دارد که همین موضوع هزینه‌های زیادی را به همراه خواهد داشت.

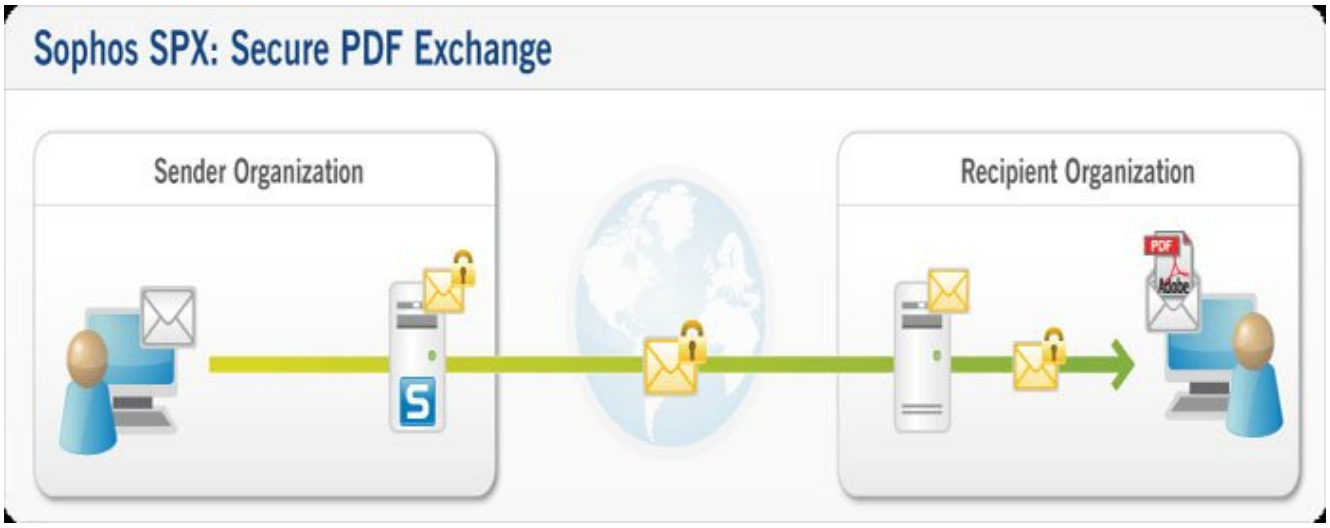
اما هر دو این فناوری‌ها دارای یک مشکل بزرگ هستند، هم فرستنده و هم گیرنده نیاز به پشتیبانی از تعویض کلیدهای عمومی برای رمزنگاری و رمزگشایی ایمن پیام‌ها دارند. در فناوری S/MIME شما به شرطی از مزیت‌های کامل آن می‌توانید استفاده کنید که طرف مقابل یک گواهی‌نامه را خریداری کرده باشد.

File encryption

رمزنگاری یک راه‌حل مفید و ایمن در زمان ارسال مجموعه‌ای از فایل‌های حساس به شمار می‌رود. رمزنگاری فایل‌ها سرعت بیشتری نسبت به رمزنگاری ایمیل دارد. رمزنگاری یک آرشیو به طور کلی از تکنیک‌های رمزنگاری متقارن و نامتقارن استفاده می‌کند. بنابراین، شما باید گذرواژه مورد نیاز را با طرف مقابل به اشتراک قرار دهید. یکی از بهترین روش‌های به‌اشترک‌گذاری این رمز با استفاده از تلفن یا اگر امکان داشته باشد، گفتن حضوری گذرواژه به شخص است. به دلیل این‌که هر دو شما به گذرواژه به اشتراک گذاشته شده اطمینان دارید، این گذرواژه نباید شکسته شود. زمانی که یک فایل زیپ رمزنگاری شده را ارسال می‌کنید؛ باید اطمینان حاصل کنید که از نسخه‌های مطمئن و به‌روز استفاده شده است. به‌دلیل این‌که نسخه‌های قدیمی فرمت زیپ از رمزنگاری‌های ضعیفی استفاده می‌کنند. اما جای تأسف است که سیستم‌عامل های ویندوز و مک هیچ‌کدام از جدیدترین نسخه‌های ایمیل AES استفاده نمی‌کنند، بنابراین لازم است تا از ابزارهای جانبی دیگری همچون سون زیپ استفاده کنید.

SPX encryption

سومین گزینه SPX (سرنام Secure PDF eXchange) نامیده می‌شود که از فناوری رمزنگاری ایمیل سوفوس Sophos استفاده می‌کند (طبیعی است فقط برای کاربران Sophos کاربرد دارد. اگر مشتری Sophos نیستید، بهتر است از این گزینه صرف‌نظر کنید). زمانی‌که کاربر یک پیام رمزنگاری شده SPX را دریافت می‌کند، به آسانی یک فایل PDF را باز کرده، گذرواژه خود را وارد کرده و محتوای ضمیمه‌ها را مشاهده می‌کند. اگر من یک ایمیل SPX را برای شما ارسال کنم، شما یک دعوت‌نامه برای ثبت‌نام روی پرتال دریافت می‌کنید، مکانی که در آن گذرواژه خود را انتخاب می‌کنید. سپس، هر ایمیل همراه با یک PDF محافظت شده با گذرواژه ارسال می‌شود. شما فقط لازم است به سایت رفته و به آن پاسخ دهید. اشکال این روش در این است که شما رکوردی برای پاسخ‌های خود در میل باکس ندارید.



SPX به آسانی قابل راه‌اندازی است، و برای کاربران گزینه راحتی به شمار می‌رود، به دلیل این‌که دریافت کننده ایمیل نیاز به چیزی بیش از باز کردن یک فایل PDF ندارد. در این روش نیاز به اشتراک‌گذاری گذرواژه وجود ندارد و همچنین نیازی به نصب برنامه کلاینت نیز وجود ندارد.

پست‌الکترونیک اجتناب‌ناپذیر

گزینه‌های امنیتی بیشتری در ارتباط با ایمیل وجود دارند؛ از قبیل ابزارهای اختصاصی که برای انتقال ارتباطات روی پروتکل HTTPS مورد استفاده قرار می‌گیرند، اما همیشه عملی نیستند. شما مجبور هستید برای مدیریت روی امنیت داده‌های خود به این ابزارهای کمک کننده اعتماد کنید. با وجود عدم امنیت، ما به استفاده از ایمیل ادامه می‌دهیم؛ به دلیل این‌که ایمیل به جزء لاینفک تجارت و کسب‌وکارهای ما تبدیل شده است و حداقل به این زودی‌ها هیچ جایگزین مناسبی برای آن پیدا نخواهد شد. اما برای این‌که ایمیل به درستی ایمن شود، باید درباره همه روش‌هایی که با استفاده از آن‌ها پست‌الکترونیک می‌تواند مورد سوءاستفاده قرار گیرد، فکر کنیم. فیلتر کردن هرزنامه‌ها کاملا ضروری است، نه فقط به خاطر این‌که در زمان صرفه‌جویی می‌کند، بلکه امنیت بیشتری در برابر حملات فیشینگ در اختیار ما قرار می‌دهد. مشتریان ایمیل‌ها نیاز به وصله‌ها نیز دارند؛ به دلیل این‌که، یک مشتری ایمیل یک محتوای غیرقابل اعتماد از اینترنت را رندر می‌کند؛ که همیشه احتمال حمل یک خطر امنیتی برای اجرای نرم‌افزارهای مخربی که با باز کردن یک ایمیل اجرا می‌شوند را دارد. شما همچنین به فناوری پیشگیری از گم شدن داده‌ها DLP (سرنام Data Loss Prevention) نیاز دارید که از ارسال داده‌هایی که نباید از طرف مردم ارسال شوند، جلوگیری به عمل می‌آورد. این فناوری بر اساس قوانین هر منطقه و دستورالعمل‌های آن منطقه قرار دارد.

تاریخ انتشار:
02 اردیبهشت 1394

نشانی منبع: https://www.shabakeh-mag.com/security/568