علی‌نصیری

رویارویی نامه‌رسان‌های الکترونیکی با PGP

تصور کنید اگر در شروع یک روز تازه و خرید روزنامه صبحتان به چنین تیتر خبری برمی‌خوردید، چه حالی داشتید «پستچی باج‌گیر، نامه‌های مردم را می‌خواند». این پستچی قبل از تحویل نامه آن را می‌خواند و دوباره در پاکت را بسته و آن‌گاه تحویل می‌داد. این شگرد نامه‌رسان خائنی بود که هزاران نامه را قبل از رساندن آن‌ها به مقصد می‌خواند تا از محتویات نامه‌ها سر دربیاورد، سپس از آن یک کپی تهیه می‌کرد تا بتواند در زمان مناسب از صاحب نامه باج بگیرد.

شاید این تیتر خبری شمارا شوکه نکرده باشد؛ اما باید به شما بگویم این اتفاق در عصر ارتباطات الکترونیکی که بیش‌تر نامه‌ها در سرتاسر جهان از طریق درگاه‌های فضای مجازی تبادل می‌شوند، در همین لحظه هم در حال رخ دادن است و سرویس‌های نامه‌رسان الکترونیکی که در اصطلاح به آن‌ها ایمیل می‌گوییم، بدون اطلاع ما تمام محتویات نامه‌های ما را کاوش و بررسی می‌کنند تا برای استفاده از مقاصد خود در حال یا آینده از آن‌ها بهره ببرند. به‌طور مثال شرکت چندملیتی گوگل که در نوع خود در بین چند شرکت اول مهم و درآمدزای نظام سرمایه‌داری جهانی قرار دارد، به‌طور خاص در حال بررسی و انباشت اطلاعات موجود در ایمیل‌های کاربران خود در سرتاسر جهان است. گوگل با پردازش این اطلاعات خام و تبدیل آن‌ها به اطلاعات ارزشمند به سود سرشاری دست پیدا می‌کند. هنگامی‌که سازمان Consumer Watchdog در سال ۲۰۱۳ میلادی از این غول اینترنتی نظام سرمایه‌داری در دادگاه کالیفرنیای آمریکا از جانب مردم به دلیل جاسوسی و نقض حریم خصوصی کاربران شکایت کرد، وکلای گوگل این‌گونه واکنش نشان دادند که تمام کسانی که از طریق سرویس جیمیل مبادرت به ارسال یا دریافت رایانامه می‌کنند نباید انتظار داشته باشند که حریم خصوصی آن‌ها حفظ شود. آن‌ها گفتند گوگل قبل از رسیدن پیام به مقصد با بررسی و پردازش تمام محتوای آن به اطلاعاتی دست پیدا می‌کند که با آن تشخیص می‌دهد چه تبلیغاتی را باید به خواننده و ارسال‌کننده آن پیام ارسال کند. البته واضح است که یکی از موارد استفاده گوگل از این اطلاعات، کسب درآمد به‌وسیله سامانه تبلیغاتی گوگل است نه تمام آن. حال تصور کنید چه اطلاعاتی توسط استادان دانشگاه، محققان، دانشمندان، سازمان‌های دولتی، NGO های خصوصی، مخالفان دولت‌ها، نظامیان، دولتمردان، کارمندان و تمام افراد یک جامعه در هرلحظه در حال تبادل است، این پیام‌ها گاه شامل اطلاعاتی است که فرستنده نمی‌خواهد جز گیرنده پیام برای فرد دیگری قابل روئیت باشد، حتی برخلاف تصور، اطلاعات افرادِ عادی هم برای این شرکت‌های چندملیتی دارای اهمیت فراوانی است. چه کسی می‌داند در آینده برایش چه اتفاقی رخ می‌دهد! پس دانستن هر اطلاعاتی از یک فرد می‌تواند نقش تعیین‌کننده‌ای در مواجهه با آینده داشته باشد. در برخی اسناد منتشرشده توسط افشاگرانِ اطلاعاتِ دولتی در آمریکا مانند ادوارد اسنودن آمده است که سرفرماندهیِ ارتباطاتِ دولتی انگلیس و آژانس امنیت ملی آمریکا سال‌هاست که در پروژه‌ای مشترک از همه ایرانیان به‌صورت ۲۴ ساعته و در هفت روز هفته جاسوسی می‌کنند.

تحلیلگران امنیتی می‌گویند به گزارش این سند اطلاعاتی، دو کشور آمریکا و انگلیس، جامعه ایران را به دو طیف مذهبی و غیرمذهبی تقسیم نموده‌اند؛ با این هدف که از افراد مذهبی مقیّد به شرعیات، اسنادی دال بر عبور از اخلاقیات و موازین اسلامی جمع‌آوری کنند و از افراد غیرمذهبی که التزامی به رعایت مسائل دینی ندارند، اما در مقابل احتمال می‌رود فعالیت‌های سیاسی ضد اسلام و نظام جمهوری اسلامی از آن‌ها سر بزند، فعالیت‌هایشان را بر ضد امنیت ملی ثبت و ضبط نمایند. پرواضح است در آینده، کلیه مسؤولیت‌های کشوری و لشکری نظام جمهوری اسلامی در اختیار نسل جوان کنونی قرار خواهد گرفت، بنابراین از هم‌اکنون دشمن کلیه افراد را زیرنظر دارد و به شیوه‌ای که بیان‌شده اطلاعات تخلفات آن‌ها را ثبت می‌کند تا هر کس در آینده به مسؤولیت‌های حساس گمارده شد، با وی معامله یک‌طرفه انجام دهد و به‌اصطلاح «گروگان‌گیری اطلاعاتی» علیه شخص مفروض صورت دهد. بدین ترتیب افراد مجبور می‌شوند برای جلوگیری از افشای اطلاعات منفی‌شان و حفظ آبروی خود، به هرگونه درخواست خیانتی از سوی دشمن تن دردهند.

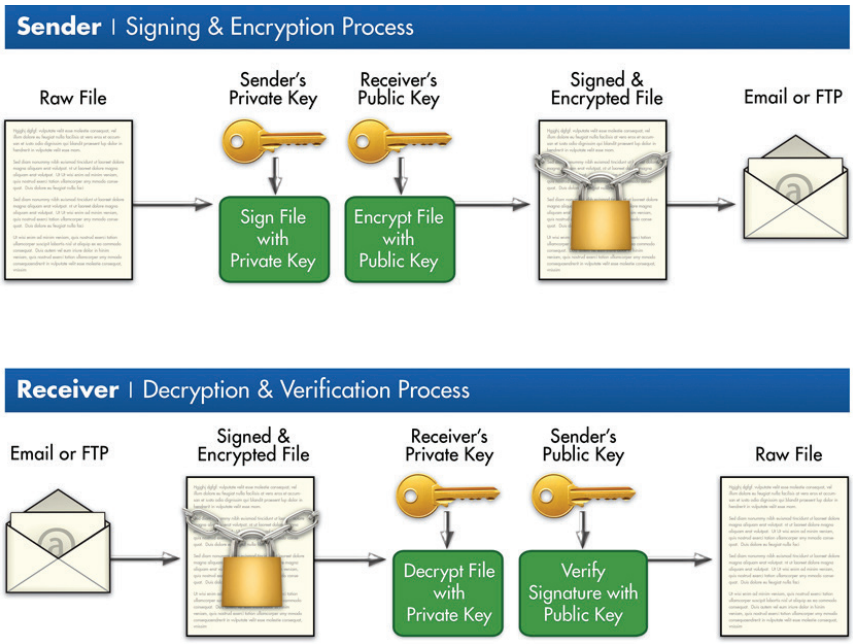
وقتی یک پیام _که می‌تواند حاوی هر اطلاعاتی باشد_ توسط پست الکترونیکی بین دو سایت راه دور مبادله می‌شود، در طول مسیر خود از ده‌ها ماشین دیگر عبور می‌کند، هر یک از این ماشین‌ها قادرند آن را بخوانند یا برای استفاده‌های بعدی ذخیره کنند. این قانون در مورد همه بسته‌های اطلاعاتی که توسط رایانه‌های شخصی یا موبایل تبادل می‌شوند نیز صادق است. برخلاف آن‌چه عموم مردم می‌اندیشند، حریم خصوصی در فضای مجازی وجود ندارد. باید آگاه باشیم که در تفکر نظریه‌پردازان غربی که اداره‌کنندگان و رهبران فکری نظام سرمایه‌داری جهانی هستند، عنصر مؤثر اصلی در عصر اطلاعات در حقیقت همان اطلاعات است که با دراختیارداشتن و پایش آن به اطلاعات مفید، می‌توانند به‌راحتی به سلطه خود برجهان ادامه دهند.

آنان بر این باورند که اولین عصر، شامل کشاورزی و تحولات انسانی مربوط به آن است. این کار، انسان را از تلاش دائم برای امرارمعاش رها ساخت و ثبات و امنیت لازم برای توسعه فنون و فن‌آوری‌ها را که مبنای تمدن امروز هستند، فراهم آورد. آنان نماد عصر کشاورزی را بیل و کلنگ می‌دانند. عصر دوم، انقلاب صنعتی است که دربرگیرنده حرکت بشر به سمت روش‌های تولیدی نوین و سازمان‌دهی نیروی کار برای بهره‌برداری حداکثری می‌باشد. جهان صنعتی مخلوق آن است. بهره‌برداری از مواد اولیه، تولید انبوه و کاربرد فزاینده‌تر فن‌آوری، رفاه و سعادت را برای کشورهایی به دنبال داشته که از عهده تغییرات لازم برآمده بودند. آنان بر این باورند که نماد عصر دوم یا انقلاب صنعتی، موتور است. عصر سوم، تحولی پس از دوران صنعتی و مبتنی بر اطلاعات است که به گفته آنان در دهه ۱۹۵۰ آغازشده است. نماد عصر سوم که گاه از آن باعنوان موج فراصنعتی نام می‌برند، رایانه است. رایانه با دریافت اطلاعات خام، آن را به اطلاعاتی درخور توجه و ارزشمند تبدیل می‌کند، شاید بتوان آن را به پالایشگاه نفت تشبیه کرد اما در عصر اطلاعات، ارزش اطلاعات هیچ‌گاه با نفت و امثال آن قابل قیاس نیست.

با توجه به این مطالب و دریافت اهمیت اطلاعات و نقش کلیدی حامل‌های آن می‌توان گفت که تیتر خبری «نقض حریم خصوصی کاربران توسط سرویس‌دهندگان پست الکترونیکی» یک تیتر شوکه‌کننده است. این در حالی است که احتمالا تیتر خبری «اطلاعات مهم ایمیل هزاران کاربر یک کافی‌نت به سرقت رفت» برای مردم و حتی مراجع امنیتِ سایبری کشورمان مانند پلیس فتا مهم‌تر باشد. تصور کنید حالِ فردی را که عکس‌های خانوادگی‌اش در فضای مجازی و شبکه‌های اجتماعی پخش شده، چگونه است؟ شاید شما بارها خبرهایی از سرقت عکس‌های خصوصی و دیگر اطلاعات مهم کاربران مانند اطلاعات حساب‌های مالی و مدارک خصوصی افراد را در خبرگزاری‌های داخلی شنیده باشید؛ یا حتی خودتان یکی از آن‌هایی باشید که مورد حمله هکرها و افراد سودجو قرار گرفته و به سبب آن، متحمل خسارت‌های روحی و مالی شده‌اید، ما باید بدانیم هم از نظر شخصی و هم از نظر امنیت ملی کشورمان در فضای مجازی در موقعیت ضعف قرار داشته و درخطر هستیم. پس در نتیجه از دیدگاه فردی و از دیدگاه میهنی به عنوان یک شهروند آگاه و مسؤولیت‌پذیر، باید تمام مراتب پیشگیرانه امنیتی را به منظور حفظ اطلاعات شخصی‌مان در درجه اول و سپس تمام اطلاعات مربوط به محل کار یا به طور عام هر آن‌چه به دیگران مربوط می شود را رعایت کنیم.

سؤال پیش روی ما این است که آیا هیچ راهی برای در امان ماندن از نشت اطلاعات شخصی خود به بیرون نداریم؟ تا به امروز به دلیل کم‌اهمیت شمردن این موضوع توسط دولت و ناآگاهی بخشی و آموزش عمومی، بسیاری از مردم از راه‌های مقابله با این تهدیدها بی‌خبر مانده‌اند و استقبال چندانی از راه‌های پیشگیری از تهدیدها نشده است. افراد زیادی از متخصصان برای ارائه راه‌کارهای امنیتی وجود دارند اما شرکت‌ها و بنگاه‌های بزرگ ترجیح می‌دهند تا بتوانند از این آب گل‌آلود به نفع خود و در جهت جمع‌آوری حداکثری اطلاعات استفاده کنند؛ درنتیجه افراد دغدغه‌مند یا تنها مانده‌اند و حمایت نمی‌شوند تا ابزارهای مناسب تولید شود، یا افراد اندکی از آن‌ها به‌صورت خودجوش دست‌به‌کارهایی می‌زنند

برخلاف آن‌چه عموم مردم می‌اندیشند، حریم خصوصی در فضای مجازی وجود ندارد. باید آگاه باشیم که در تفکر نظریه‌پردازان غربی که اداره‌کنندگان و رهبران فکری نظام سرمایه‌داری جهانی هستند، عنصر مؤثر اصلی در عصر اطلاعات در حقیقت همان اطلاعات است که با دراختیارداشتن و پایش آن به اطلاعات مفید، می‌توانند به‌راحتی به سلطه خود برجهان ادامه دهند.



که آن‌ها هم غالبا به دلیل کمبود منابع مالی برای تبلیغات کم‌تر مورد استفاده و آزمون قرار می‌گیرند. یکی از بهترین روش‌های پیشگیرانه به منظور مقابله با نقض حریم خصوصی نامه‌های الکترونیکی و اطلاعات خصوصی، رمزنگاری آن‌ها است؛ به‌طوری‌که با این عمل تنها صاحب محتوا و مخاطبان مجاز تعریف شده آن می‌توانند به آن‌ها دسترسی داشته باشند.

سال‌ها پیش از امروز آقای فیل زیمرمان آمریکایی به‌صورت کاملاً شخصی دست به ساخت نرم‌افزاری ساده اما کاربردی زد تا بتواند جلوی نشت اطلاعات شخصی موجود در نامه‌های الکترونیکی را بگیرد و همه مردم بتوانند به‌صورت رایگان از آن استفاده کنند، او نام این نرم‌افزار را PGP گذاشت، از اولین روز معرفی PGP در سال ۱۹۹۱ بحث‌وجدل‌های فراوانی پیرامون آن شکل گرفت تا آن‌جا که دولت ایالات‌متحده او را متهم ساخت که قوانین «منع صدور ابزارهای استراتژیک» را نقض کرده است، بازجویی و رفت‌وآمد زیمرمان در دادگاه پنج سال طول کشید اما سرانجام پرونده وی مختومه اعلام شد. شعار او که یکی از طرفداران حفظ حریم خصوصی افراد در فضاهای مجازی است این بود: «اگر حفظ حریم خصوصی و حفظ اسرار مردم، قانون‌شکنی است، آن‌گاه فقط حریم خصوصی قانون‌شکنان حفظ خواهد شد.» زیمرمان با ساخت این نرم‌افزار توانست خود را به پدر نرم‌افزارهای امنیتیِ پست الکترونیکی تبدیل کند؛ به همین سبب، او از مؤسسات و نهادهای مردمی نیز جوایز و تقدیرنامه‌هایی دریافت کرد. امروزه از وی به دلیل خدماتش به نیکی یاد می‌شود، همچنین زیمرمان بعدها در شرکت‌های مستقل بسیاری دست به ساخت و توسعه ابزارهای رمزنگاری به‌منظور امن‌سازی اطلاعات پست‌های الکترونیکی زد. او حتی یک سرویس‌دهنده ایمیل امن ساخت تا کاربران آن بدون نگرانی به دریافت و ارسال نامه‌های خصوصی خود بپردازند، اما طولی نکشید که این سرویس و تمام سرویس‌های مشابه به دستور دولت آمریکا خاموش شدند تا امروز هیچ شرکت مستقلی وجود نداشته باشد که خدمات امن سرویس پست الکترونیکی را به مردم آمریکا ارائه کند؛ چراکه دولت امریکا از وی خواسته بود تا تمام ایمیل‌ها را شنود کند. زیمرمن اعلام کرده است با یک گروه متخصص در حال ساخت یک موبایل امن برای استفاده عموم است. او می‌خواهد با استفاده از هسته سیستم‌عامل اندرونید و با اصلاح حفره‌های فراوان امنیتی آن، دست به ساخت یک موبایل هوشمند امروزی بزند؛ چراکه پیش‌بینی می‌شود در چند سال آتی سرقت و جاسوسی اطلاعات از موبایل‌های شخصی افراد، بزرگ‌ترین چالش پیش روی مردم جهان در دنیای مجازی باشد.

اساس کار PGP بر رمزنگاری داده‌ها با الگوریتم‌های موجودی بود که توسط مؤسسات و نهادهای غیروابسته به دولت ساخته‌شده بودند، برای افرادی که به دولت اعتماد ندارند این‌یک امتیاز محسوب می‌شود. در حال حاضر اصول PGP به یک استاندارد بین‌المللی برای ابزارهای رمزنگاری تبدیل‌شده است، تاکنون نسخه‌های فراوانی از روی این استاندارد برای استفاده عموم ساخته‌شده‌اند. این نرم‌افزارها اغلب با تمام سیستم‌های عامل ازجمله ویندوز و حتی دستگاه‌های موبایل اندرویدی سازگاری دارند و بسیاری از مردم جهان از آن‌ها استفاده می‌کنند. برای استفاده رایگان و یادگیری نرم‌افزار کاربردیِ PGP کافی است نام این نرم‌افزار را در موتورهای جستجو بنویسید تا هر آن‌چه لازم دارید برایتان حاضر شود، و یا مستقیم به سایت شخصی آقای زیمرمان به نشانی www.philzimmermann.com مراجعه کنید و به کسب اطلاعاتی در مورد انواع نرم‌افزارهای ساخته‌شده با استاندارد PGP بپردازید. این نرم‌افزار پس از ساختن یک کلید عمومی برای رمزنگاری داده‌ها _ که از آن به‌عنوان امضای دیجیتال یاد می‌شود_ می‌توانید نامه های الکترونیکی‌تان را رمز کرده و ارسال کند، همچنین می‌توانید هر نوع فایل بااهمیت از نظر خودتان را با این برنامه رمزگذاری و در هنگام لزوم با برداشتن رمز، از آن استفاده کنید.

در کشور ما نیز وجود سرویس‌های ایمیل امن و نرم‌افزارهای رمزنگاری بومی، بسیار ضروری است، چراکه در نبود زیرساخت‌های سخت‌افزاری، پروتکل‌ها و استانداردهای بومی لازم برای امن‌سازی لایه‌های زیرین سخت‌افزاری که نقش اساسی و تعیین‌کننده‌ای در امنیت داده‌ها دارند، سریع‌ترین و کم‌هزینه‌ترین راه، ساخت و استفاده از نرم‌افزارهایی مانند PGP است. در غیر این صورت باید شاهد به تاراج رفتن اطلاعاتی باشیم که پیش‌تر آن را به نفت خام تشبیه کردیم؛ نفت خامی که پالایشگاه‌های اطلاعاتی بزرگی مانند گوگل و مایکروسافت را تغذیه کرده و ما را برای همیشه مستعمره آن‌ها نگاه می‌دارد.