عوامل اطمینان‌یابی از ایمنی و تجارت الکترونیکی

نوشته: *Chidambaram Mahadevan*
ترجمه: سیروس متین‌رزم

تجارت الکترونیکی

تجارت الکترونیکی موجب تغییرات عمده‌ای در امور تجاری گردیده است. این تجارت تا حد امکان، از طریق شبکه انجام می‌گیرد: خواه پرداخت یک صورت حساب، خواه سفارش یک پیتزا. برای انجام تمام این کارها از طریق شبکه شما به امکانات زیربنایی شامل رایانه‌های میزبان، سیستم‌های عامل، کاربردها، ارتباطات نرم‌افزاری و بزرگ‌ترین شبکه‌ی جهانی، یعنی اینترنت، نیاز دارید. شما به خدمات پشتیبانی از جمله ارائه‌کنندگان خدمات ارتباطی که انجام کارها را از طریق شبکه میسر می‌سازند، نیاز دارید.

آن دسته از واحدهای تجاری که اساساً خدمات را ارائه می‌کنند و به شبکه متصل‌اند در قبال مشتریانشان مسئول‌اند و باید خدمات خود را به مشتریانشان به صورت مطمئن عرضه نمایند. با توسعه‌ی روزافزون شبکه‌ها در سراسر جهان برای انجام ماموریت‌های مهم تجارت الکترونیکی، ایمن‌سازی شبکه‌ها از اولویت اول برخوردار خواهد بود.

درحالی که ایمنی سیستم‌های عامل، کاربردها و ایمنی فیزیکی مورد توجه سازمان‌ها هستند، حوزه‌هایی که در معرض ریسک قرار دارند، شبکه‌ها و خطوط ارتباطی است که از حیطه‌ی کنترل سازمان‌ها خارج است. ایمنی یک نیاز اساسی برای کاربردهای تجارت الکترونیکی مانند پست الکترونیکی (e-mail)، سفارش‌های خرید، ارسال اطلاعات اعتباری و خودکارسازی استفاده از فرم‌های امضا شده می‌باشد.

این مقاله سعی دارد مفاهیم پایه‌ای و فن‌آوری‌های متداولی را معرفی کند که معاملات تجاری را ایمن می‌کنند.

خطرات احتمالی تجارت الکترونیکی

هر معامله یا پیامی، اعم از مالی یا غیرمالی در معرض خطر قرار دارد. در یک محیط متداول تجاری، راه‌های زیادی وجود دارند تا بتوان این خطرات را با کمک امضاءهای رسمی و سازوکارهای دیگر که ضامن معاملات مطمئن‌اند ردیابی نمود. خطرات و مسائل عمده‌ای که رو در روی محیط‌های تجارت الکترونیکی است عبارت‌اند از:

- هویت یا اعتبار شخص ـ چه کسی پیام را فرستاده؟ آیا فرستنده اختیار ملزم و متعهد کردن سازمانی را که نماینده‌ی آن می‌باشد دارد؟
- صحت داده‌ها ـ آیا پیام کامل است؟ آیا در طول مسیر تغییر کرده و آیا می‌توان ثابت نمود که پیام تغییر نکرده است؟
- عدم ارائه‌ی سرویس ـ وقوع حمله‌ی رایانه‌ای که ارائه‌ی سرویس را با شکست مواجه می‌کند.
- تایید پیام ـ اثبات پیام در دادگاه، تضمین این که فرستنده‌ی پیام نمی‌تواند ارسال پیام و یا محتویات آن را به دروغ انکار نماید.
- محرمانه بودن ـ تضمین این که اطلاعات برای افراد غیرمجاز فاش نمی‌شود.

اجزای اصلی ایمنی ارتباطات

اجزای اصلی ایمنی ارتباطات عبارتند از:

۱- رمزنویسی،
۲- گواهینامه‌های رقمی.
۳- مراجع کسب گواهینامه.

رمزنویسی

رمزنویسی یکی از فنون پنهان‌سازی است که به دوران **ژولیوس سزار** برمی‌گردد، کسی که به‌خاطر استفاده از فنون پنهان‌سازی برای رساندن پیام‌ها به فرماندهان نظامی‌اش معروف است. پنهان‌سازی، فنی برای تغییر پیام (دادگان یا اطلاعات) به شیوه‌ای غیرقابل تشخیص است، به‌طوری که یک دریافت‌کننده غیرمجاز قادر به کشف آن نباشد و برعکس آشکارسازی فنی برای رمزگشایی پیام به شکل اولیه است. پیام‌ها توسط یک **کلید**، پنهان و آشکار می‌شوند. این کلید می‌تواند با استفاده از یک خوارزمیک (الگوریتم) به‌صورت مقدار عددی برای تغییر دادن اطلاعات یا بالعکس مورد استفاده قرار گیرد. مدیریت کلیدها بسیار مهم است و ایمن نگاه داشتن کلیدها بزرگ‌ترین چالش ایمن‌سازی است دو سیستم برای رمزنویسی وجود دارد:

الف - رمزنویسی کلید متقارن.
ب - رمزنویسی کلید عمومی.

رمزنویسی کلید متقارن

در اکثر اوقات این سیستم مانند یک گاوصندوقی است که دو نفر از یک کلید مشابه -که کلید مخفی، شخصی یا منفرد نیز نامیده می‌شود - برای باز و بسته کردن آن استفاده می‌کنند. مشکل در ارسال مطمئن کلید به دریافت‌کننده پیام می‌باشد، به‌خصوص اگر فرستنده و گیرنده‌ی پیام از نظر جغرافیایی با هم فاصله داشته باشند. سیستم کلید منفرد می‌تواند برای یک جمع کوچک که تبادل پیام می‌کنند مفید واقع شود ولی چنانچه تبادل پیام به یک جمع در سطح یک موسسه‌ی بزرگ وسعت یابد، مدیریت کلیدها و حفظ محرمانه بودن آنها می‌تواند کار توان فرسایی باشد.

رمزنویسی کلیدعمومی

رمزنویسی با استفاده از کلید عمومی مانند روش شخص یا شرکتی است که می‌خواهد از نظر مشتریان خود بدون آن که هویتش فاش شود استفاده کند. برای این کار از صندوق‌پستی استفاده می‌نماید و شماره‌ی صندوق پستی در اختیار عموم گذاشته می‌شود. رمزنویسی کلید عمومی اولین بار توسط ریاضیدانان دانشگاه MIT در سال ۱۹۷۰ برای رفع نقایص روش کلید منفرد و مدیریت کلیدها ارائه شد. کلید شخصی می‌تواند اطلاعاتی راکه به‌وسیله‌ی کلید عمومی پنهان‌سازی شده، آشکار نماید. این جفت کلید به لحاظ محاسباتی با هم مرتبط‌اند اما هیچ یک از آنها را نمی‌توان مستقیماً برمبنای دیگری محاسبه کرد. هر دو کلید می‌توانند پیام‌ها را پنهان کنند، در حالی که فقط یکی از آنها قادر به آشکارسازی پیام است.

کلیدها به‌صورت مجموعه‌ای از علائم الکترونیکی هستند که در دیسک گردان‌های رایانه‌های شخصی ذخیره می‌شود یا به‌صورت blipهای دادگانی، روی خطوط تلفن و مطابق با استانداردهای صنعت منتقل می‌شوند. محاسبات پیچیده‌ی پنهان‌سازی و آشکارسازی پیام‌ها، به‌وسیله‌ی رایانه انجام می‌شود و کاربران درگیر این پیچیدگی‌ها نمی‌گردند.

کلید عمومی خطرات را به میزان زیادی کاهش می‌دهد، اما کاربران معتقدند موارد ضعف معدودی نیز دارد:

- اگر کلیدها گم شوند چه اتفاقی می‌افتد؟ آیا باز می‌توان پیام‌ها را آشکار نمود؟
- چه دلیلی وجود دارد که کلیدهای استفاده شده تغییر نیافته و قابل اعتماد باشند؟ آیا کسی هست که به دروغ وانمود کند صاحب آنهاست؟

● باید یک پیام مشابه که در طول شبکه به افراد مختلف ارسال می‌شود یک بار پنهان شود، آیا واقعاً همین‌طور است؟

امضاهای رقمی برای ارتباط بین گروه‌های کاربر پذیرفته شده‌اند و ممکن است این ضعف‌ها را برطرف کنند. در اینجا به ذکر مشخصات امضاءهای رقمی می‌پردازیم.

امضاءهای رقمی

امضاءهای رقمی یکی از اجزای مهم گواهینامه‌های رقمی هستند. برخلاف تصور عمومی، امضای رقمی یک امضای درست نوشته یا اسکن شده، نام یک شخص یا کد مخفی نیست، بلکه امضاءهای رقمی تبدیل اطلاعات با استفاده از رمزنویسی کلید عمومی می‌باشند که مستنداند و قابل تکثیر نیستند، هم چنین از سطح بالایی جهت تامین امنیت برخوردارند به طوری که جعل آنها غیرممکن است و در بعضی از کشورها نیز قانوناً پذیرفته شده‌اند.

مراحل ایجاد امضاءهای رقمی

همان طور که می‌دانید اعداد به‌صورت دودویی در رایانه وارد می‌شوند و می‌توانند به عنوان معادله‌های ریاضی تلقی گردند که در نتیجه‌ی مجموعه‌ای از عملیات به شکل نمایش منحصر به فردی ظاهر می‌گردند.

مثلاً:

بااستفاده از خوارزمیک (الگوریتم) درک ایمن (SHA) تولید شده ← ۱۰۰۰ پیام

۳×تابع درک پیام

با استفاده از کلید شخصی

۳۰۰۰ درک پیام

تولیدشده ۴×تابع امضا

۱۲۰۰۰ امضای رقمی

امضاءهای رقمی طی چهار مرحله به شرح زیر ایجاد می‌گردند:

● یک برنامه‌ی منبع از طریق تابع ریاضی یک طرفه اجرا می‌گردد (درک پیام).

● این تابع یک رقم با طول ۱۲۸ بیت برای تمام و هر یک از برنامه‌های ورودی ایجاد می‌کند که همان تابع درک پیام یا hash است.

● درک پیام با استفاده از کلید شخصی کاربر پنهان‌سازی می‌گردد.

● کلید شخصی توسط امضاکننده، رمزگذاری می‌گردد و به انتهای برنامه پیوست می‌شود و بلوک امضای رقمی حاصل می‌آید.

خوارزمیک (الگوریتم) درک پیام در امضاءهای رقمی کارگذاشته شده و در بسته‌های نرم‌افزاری شرکت‌هایی مانند xCert و Baltimore Technology ساخته می‌شوند، مرورگرهای اینترنت microsoft و Netscape نیز قادر به تولید جفت کلیدهای یاد شده روی رایانه‌ها می‌باشند. یکی از توابع متداول درک پیام، تابع MD5 مربوط به شرکت RSA است که بیشتر اوقات از این تابع استفاده می‌شود. این تابع یک سویه است و به همین دلیل پیام اولیه نمی‌تواند از روی درک پیام ساخته شود.

هر پیام جدید یک امضای رقمی متفاوت دارد، درست برخلاف امضاءهای سنتی که یک فرستنده از یک امضای مشابه برای همه‌ی نامه‌هایی که می‌فرستد، استفاده می‌کند.

اکنون با فرض تشکیل امضای رقمی می‌بینیم که چگونه اطلاعات آشکار می‌گردند. پس از تشکیل بلوک امضای گیرنده‌ی اطلاعات با استفاده از کلید عمومی فرستنده، برعکس رویه‌ی ایجاد امضای رقمی عمل نموده و آشکار می‌شوند. این‌کار منجر به درک پیام شده و علاوه برآن دریافت کننده، اعتبار امضای رقمی را نیز بررسی می‌کند. به این ترتیب که هم زمان با استفاده از خوارزمیک (الگوریتم) درک پیام، درک پیام دیگری محاسبه می‌شود و با درک پیام دریافت شده در مرحله‌ی اول مقایسه می‌گردد. اگر با هم یکی بود، محرز می‌شود که پیام تنها توسط فرستنده ارسال شده است.

در واقع، کار دریافت‌کننده جز انتخاب یک کلید بر روی دکمه‌ی تایید امضاء انجام نمی‌دهد و نرم‌افزار تمامی محاسبات ریاضی را انجام می‌دهد و مشخص می‌نماید که امضاء معتبر است یا خیر؟

گواهینامه‌های رقمی

گواهینامه‌های رقمی، گواهینامه‌هایی هستند که امضای رقمی، کلیدهای عمومی و خوارزمیک (الگوریتم) درک پیام را به طرف‌های مشخص یک مبادله تجاری معرفی می‌کنند و توسط مراجعی نظیر Entrust و Verisig که اجازه‌ی صدور گواهینامه‌های رقمی را دارند صادر می‌گردند. گواهینامه‌های رقمی از قسمت‌های زیر تشکیل گردیده‌اند:

● نام امضاء کننده.

● تاریخ انقضای گواهینامه.

● کلید عمومی امضاء کننده.

● امضای رقمی مرجع صدور گواهینامه.

● کلید عمومی مرجع صدور گواهینامه.

● خوارزمیک (الگوریتم) استفاده شده در پنهان‌سازی.

هر گواهینامه یک کلید عمومی را به یک فرد یا هویتش مرتبط نموده و در یک **انباره‌ی برخط** ذخیره می‌کند. هر فرستنده و گیرنده‌ای می‌تواند برای کسب گواهینامه‌های رقمی از مراجع صدور گواهینامه‌های رقمی اقدام نماید. گواهینامه‌های رقمی با صرف هزینه‌ای معقول برای تبادلات پست الکترونیکی و از

طریق خطوط اینترنت می‌توانند برای یک دوره‌ی زمانی مشخص، صادر و تمدید گردند.

زیربنای کلید عمومی (PKI)

PKI[1] ، فرایند مدیریت کلیدها، صدور و ردیابی، کنترل لغو کلیدها و صدور گواهینامه به صورت سازماندهی شده و صحیح، جهت اجرای آسان ارسال و دریافت پیام می‌باشد. مسئولیت صدور گواهینامه‌های رقمی با مراجع صدور گواهینامه (CA)[2] می‌باشد. یک PKI جامع و کامل باید شامل منابع و توانایی‌های زیر باشد:

- مرجع گواهینامه ـ شخص ثالث و معتمدی است که مسئولیت صدور گواهینامه و پشتیبانی کلیدهای عمومی را به‌عهده دارد.
- ایجاد یک محل ـ برای نگهداری گواهینامه‌های صادر شده به طوری که بتوان در صورت لزوم صحت و سقم گواهی‌ها را بررسی کرد.
- سازوکارهای کنترلی ـ جهت کنترل، ابطال و یا تمدید گواهینامه پس از طی دوره‌ی انقضا.
- یک سیستم پشتیبان ـ برای کاربرانی که رمز عبور خود را برای رمزگذاری و معتبر نمودن امضای رقمی جهت تکمیل مبادله فراموش کرده‌اند.
- صدور گواهینامه ـ برای گواهینامه‌های رقمی که اعتبارشان تائید شده است.
- فرایند ایجاد اطمینان ـ نسبت به گواهینامه‌هایی که ازمحدوده‌ی مقررات خارج گردیده‌اند.

مراحل کسب گواهینامه‌ی رقمی

کسب یک گواهینامه‌ی رقمی بدین ترتیب است که یک امضاءکننده، درخواست خود را برای مراجع صدور گواهینامه (CA) ارائه می‌کند. CA اعتبارنامه و مشخصات هویتی درخواست کننده را بررسی می‌کند و پس از ارزش‌یابی و تایید مدارک، گواهینامه‌ی رقمی صادر می‌کند. گواهینامه‌ی رقمی سریعاً به انباره‌ی برخط فرستاده می‌شود و تقاضادهنده نیز با مراجع به این انباره، گواهینامه‌ی خود را دریافت و با استفاده از کلید عمومی CA، نسبت به آشکارسازی اقدام می‌نماید.

امضاهای رقمی و لوایح و قوانین

علاوه بر اقدامات ایمنی بحث شده، قوانین و احکامی نیز برای پشتیبانی و حمایت از انجام تجارت الکترونیک لازم می‌باشد. بسیاری از کشورها قوانین لازم را تصویب یا نسبت به تصحیح قوانین پیشین خود اقدام نموده‌اند. لذا شرکت‌هایی که مایل‌اند وارد عرصه‌ی تجارت الکترونیک شوند باید برای مقابله با خطرات احتمالی، اقدامات لازم را انجام دهند یکی از راه‌های جلوگیری از ضررهای احتمالی تجارت الکترونیکی این است که طرفین معامله، اشخاص ثالث و شرکت‌های بیمه برای حق بیمه به توافقی برسند تا تعهدات آنها در مقابل کاستی‌ها به یک مبلغ به‌خصوصی محدود گردد.

هم چنین توصیه می‌گردد که این شرکت‌ها واحد حسابرسی داخلی و متخصصین حسابرسی سیستم داشته باشند تا تجارت الکترونیکی پیشنهادی را مستقلاً بازبینی کنند.

پی‌نوشت

1- PKI = Public Key Infrastructure

2- CA = Certificate Authority ■