مدل‌سازی اعتماد در بانکداری اینترنتی

محمود درودچی– استادبخش کامپیوتر دانشگاه کاردینال استریچ امریکا (Mdoroodchi@gmail.com)
آزاده ایرانمهر– دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات، دانشگاه شیراز (Iranmehr@gmail.com)

بخش پایانی

اشاره

در بخش‌های قبلی این مقاله، ضمن مروری بر موضوع اعتماد در بانکداری اینترنتی، به آنالیز گردش اطلاعات در بانکداری اینترنتی و ریسک‌های موجود پرداختیم و اجزای مختلف مؤثر در ایجاد و افزایش اعتماد نسبت به وب سایت‌های بانکداری اینترنتی را برشمردیم و تکنولوژی‌های مؤثر در این رابطه (همچون حریم خصوصی و محرمانگی، در دسترس بودن، صحت داده‌ها، احراز هویت و تصدیق اصالت) را تشریح کردیم، و اینک به ادامه بحث درباره سایر تکنولوژی‌های مؤثر بر این امر می‌پردازیم.

بانک و اقتصاد

* کنترل دسترسی: در انجام هر تراکنش مالی، هر مشتری باید بتواند در حدی که مجاز است، تراکنش مالی انجام دهد. به عنوان مثال، هیچ پولی نباید به مشتری پرداخت شود مگر اینکه کاملاً مطمئن شویم که تمام شرایط پرداخت را براساس هویتی که قبلا شناسایی شده است، دارا می‌باشد، و مجاز به برداشت حجم معینی است که از قبل برای او تعریف شده است. کنترل دسترسی، معمولاً به صورت جداول کنترل دسترسی برای هر مشتری براساس سیاست‌های بانک مورد نظر تعیین می‌شود[۶].

* انکار ناپذیری: در هر تراکنش، طرفین معامله باید جهت انجام معامله، مورد حسابرسی قرار گیرند، یعنی آن‌ها نباید قادر باشند حضور خود را در آن معامله انکار کنند. برعکس، همانگونه که موجودیت‌ها نباید بتوانند حضورشان را در معامله انکار کنند، در صورتی که واقعاً در معامله‌ای شرکت نکرده‌اند، باید قادر باشند عدم حضور خود را نیز اثبات کنند. انکار ناپذیری، قدرت انکار را مینیمم می‌کند، ولی باعث کاهش گمنامی و افزایش ریسک‌های مربوط به شکسته‌شدن حریم خصوصی می‌شود[۱۶و۱۷].

توابع در هم‌ساز (Hash Function)، کارت هوشمند، امضای دیجیتالی، گواهی‌های دیجیتال و سیستم‌های ثبت وقایع، از جمله تکنیک‌های ایجاد انکارناپذیری می‌باشند، که از الگوریتم رمزنگاری نامتقارن و در هم‌ساز (Hash Algoritms) استفاده می‌کنند[۶].

* نظارت و گزارشگیری: سیستم‌های مربوط به نظارت (Monitoring) می‌توانند دسترسی‌های غیر مجاز به سیستم‌های کامپیوتری و حساب‌های مشتری را تشخیص دهند. یک سیستم احراز هویت، تشخیص اصالت و انکار ناپذیری مناسب باید شامل امکانات بازرسی و حسابرسی نیز

باشد، که بتواند به تشخیص تهاجمات، شستشوی پولی، به خطر افتادن رمز عبور و سایر فعالیت‌های غیر مجاز کمک کند. ثبت و نگهداری وقایع (Audit Log) باعث تشخیص فعالیت‌های غیرمجاز، تشخیص نفوذ، بازسازی وقایع و ترفیع حسابرسی کارمندان و کاربران می‌شود. علاوه بر این، مؤسسات مالی باید بتوانند فعالیت‌های مشکوک را به مراکز و نمایندگی‌های قانونی گزارش کنند. مؤسسات مالی هم باید بر روی لایه‌های چند گانه کنترل برای جلوگیری از کلاهبرداری و حفاظت از اطلاعات مشتریان تکیه کنند. بیشتر این کنترل‌ها مستقیماً بر پایه تصدیق اصالت و احراز هویت نمی‌باشند. به عنوان مثال، یک مؤسسه مالی می‌تواند فعالیت مشتریانش را برای تشخیص الگوهای مشکوک آنالیز کند. مکانیسم گزارشگیری مناسب برای اطلاع‌رسانی به مدیران نیز لازم می‌باشد. خصوصاً اگر سیستم‌ها و فرآیندهای حساس به شرکت‌های ثالث داده شود، مدیران باید اطمینان حاصل کنند که توابع نظارت و گزارشگیری مناسب در حال اجرا می‌باشد و فعالیت‌های غیرمجاز و مشکوک در زمان های بخصوصی با بانک ارتباط ندارند، و یک عضو غیر وابسته (مثل بازرس های داخلی و خارجی) گزارش‌های فعالیت را بازبینی و عملکرد مدیران امنیتی را جهت اعمال کنترل های لازم و توازن سیستم مدیریت امنیتی ثبت کند[۱۸ و ۶].

چنانچه مشاهده می‌کنید، روش‌های ایجاد اعتمادی که بر پایه امنیت قرار دارند، بر پایه و اساس PKI و CA استوار می‌باشند.

۴-۲-۲) کارایی: وقتی که یک برنامه کاربردی در یک محیط عملیاتی مثل اینترنت اجرا می‌شود، عملکردش با آنچه در طول ایجاد برنامه مشاهده می‌شود، تفاوت می‌کند.

وقتی که تعداد زیادی از کاربران تلاش می‌کنند که به وب‌سایت دسترسی داشته باشند، به دلیل افزایش تقاضا برای پهنای باند و منابع سرویس دهنده، عملا کارایی پایین می‌آید. هنگامی که در سمت سرویس‌دهنده، مصرف منابع تا سطوحی که در طول طراحی ملاحظه نشده افزایش یابد، در سمت مشتری، زمان پاسخ (از لحظه‌ای که مشتری بر روی موس کلیک می‌کند تا زمانی که صفحه وب کاملاً بر روی صفحه نمایش داده می‌شود) مسأله قابل بحثی خواهد شد[۸].

بانک‌ها باید مطمئن شوند که صفحات وبشان بر روی اینترنت به خوبی کار می‌کند. برای رسیدن به یک کارایی مورد قبول، فاکتورهایی مثل متوسط سرعت بارگذاری و بالاگذاری یک وب‌سایت، شرایط ایجاد ترافیک، دسترسی به پایگاه داده، زمان پردازش، بهینه‌سازی منابع سرویس‌دهنده و سرعت اتصال قابل قبول برای مشتریان، باید با دقت زیاد مطالعه و آزمایش شوند.

۴-۲-۳) مقیاس پذیری: زمانی که تعداد زیادی از کاربران به طور همزمان بخواهند به وب‌سایت دسترسی پیدا کنند، ممکن است که یک یا تعداد بیشتر منابع مربوط به آن سرویس‌دهنده، اشباع شود و جلسه فعال آن سرویس‌دهنده با مشتری قطع و یا آن سرویس‌دهنده از سرویس خارج شود. در نتیجه، وب سایت قادر نخواهد بود که درخواست کاربران را به خوبی پردازش کند، و متوسط زمان پاسخ افزایش می‌یابد[۸]. زمانیکه چنین اتفاقی می‌افتد، مشتریان نظرشان نسبت به سایت تغییر می‌کند و به سوی سایت‌های رقیب می‌روند. بنابراین، برای هر وب‌سایت این مسأله مهمی است که بتواند از تغییرات ایجاد شده در تعداد کاربران همزمان پشتیبانی کند.

یک وب‌سایت برای اینکه بتواند تمام درخواست‌های مشتریان را به صورت تراکنش‌های امن انجام دهد و یا اینکه از هر گونه تغییری در تعداد کاربران همزمان پشتیبانی کند، منابع محاسباتی را به زیرساخت‌های تکنولوژی خود اضافه می‌کند. این قابلیت را مقیاس‌پذیری می‌نامند[۵].

روش دیگری نیز وجود دارد که در ۱۱ سپتامبر سال ۲۰۰۱ در بیشتر سایت‌های خبری از آن استفاده می‌شد. در

آگاه‌سازی مشتریان، کلید اصلی دفاع در برابر کلاهبرداری‌ها و سرقت هویت می‌باشد.

وجود خواهد داشت. بنابراین، جهت افزایش اعتماد مشتریان، سیستم‌های پرداخت باید شامل موارد زیر باشند[۲۰]:

* استفاده از نظام‌های پرداخت فاقد نام (No Name) جهت گمنامی (Anonymity) کاربران و پرداخت‌کنندگان.
* استفاده از نظام‌هایی که در آن‌ها محل انجام تراکنش پرداخت قابل شناسایی نباشد (UntraceabilityLocation).
* استفاده از نظام‌هایی برای اینکه دو تراکنش مالی نتوانند با یک مشتری برقرار شوند (Untraceability Payment Transaction).
* استفاده از تکنیک‌های رمزنگاری و محرمانگی که به صورت انتخابی و دلخواه از افشای داده‌های مربوط به تراکنش پرداختی جلوگیری کنند.
* استفاده از سرویس‌های انکارناپذیری در دستورهای پرداخت جهت جلوگیری از انکار آنچه واقعا رخ داده است.
* امکان تازه‌سازی پیام‌های مربوط به دستور پرداخت جهت جلوگیری از حملات تکرار.

۴-۴) شرح کامل فعالیت بانک‌ها به مشتریان: یک بانک تحت وب، مسوول تمام اطلاعاتی است که بر روی وب‌سایتش گردآوری کرده است، همچنانکه مسوول انجام هر تراکنشی می‌باشد که بر روی آن انجام می‌شود. یک بیننده متوجه نخواهد شد که آیا آنچه او از وب سایت بدست آورده، حقیقت داشته یا نه؟ آیا بانک واقعاً قصد دارد آن تعهداتی را که در سایت بیان کرده، انجام دهد یا نه؟ یا آیا اطلاعاتی که مشتری در سایت درج کرده، محرمانه باقی می‌ماند یا نه؟ برای مینیمم کردن ریسک مشتریان نسبت به سایت و ایجاد اعتماد، وب‌سایت بانک باید تمام شرایط و عملکردهای خود را در سایت درج کند که شامل موارد زیر می‌باشد:

* شرایط پرداخت و انجام تراکنش‌های مالی: باید تمام شرایط انواع پرداخت‌های بانکی و انجام هرگونه تراکنشی از سوی مشتریان در آن به وضوح بیان شده باشد.
* شرایط ضمانت: جبران زیان مشتریان، در صورت ایجاد هرگونه ضرر و زیان از سوی بانک‌ها.
* سیاست‌های حریم خصوصی: بانک‌ها باید به صورت کاملاً واضح مقصد تمام اطلاعات شخصی را که از مشتری بر روی وب‌سایت جمع‌آوری می‌کنند، مشخص کنند.
* امکان مشورت: اگر بانک‌ها بخواهند هر نوع استفاده اضافه‌ای از اطلاعات مشتریان داشته باشند (مثلاً آن را در اختیار طرف‌های ثالث قرار دهند)، باید جهت کسب اجازه از مشتریان، سوال شود و آنها را از عواقب کار آگاه کنند.
* اعتبار (Certification Authority): CA اطلاعات کافی در مورد اعتبار CAای که بانک مورد نظر جهت گواهی‌ها و امضای دیجیتالی و تمامی مسایل مربوط به محرمانگی و رمزنگاری از آن استفاده می‌کند، باید در سایت موجود باشد.

۵-۴) شهرت و اعتبار بانک: شهرت را می‌توان به عنوان اعتقاد مشتریان همراه باسطحی معین از رضایت نسبت به یک شرکت، سازمان و یا محصولات و خدمات آن تعریف کرد. شهرت، یکی از مهمترین عوامل در ایجاد اعتماد در مشتریان نسبت به شرکت، سازمان یا محصولات و خدمات بانکی می‌باشد.

در صورتی که بانک مورد نظر در دنیای واقعی صاحب خوش‌نامی، اعتبار و سوابق مالی مناسب باشد، انتقال این اعتبار بر روی وب کار ساده‌ای است، مخصوصاً زمانی که مشتری برای اولین بار به سایت مورد نظر مراجعه می‌کند. در مواقعی که هیچ بانکی در عالم واقعی وجود ندارد، آنها نیز می‌توانند برای وب سایت خود بر روی وب اعتبار ایجاد کنند و خدمات متنوع را با همان کیفیتی که در بانک سنتی وجود دارد، ارایه دهند، هر چند که این کار وقتگیر و پیچیده‌ای است و می‌توان آن را از طریق طرف‌های سوم مورد اعتماد و ایجاد زیر ساخت‌های کلید عمومی (PKI/CA) میسر کرد.

۶-۴)آگاه‌سازی مشتریان (Customer Awareness): مؤسسات مالی باید تلاش خود را در جهت آموزش مشتریان ادامه دهند، زیرا آگاه‌سازی مشتریان، کلید اساسی دفاع در برابر کلاهبرداری‌ها و سرقت هویت می‌باشد. مدیران باید برنامه‌ای را جهت آموزش مشتریان ایجاد و به صورت مداوم کارایی آن را ارزیابی کنند. از روش‌های ارزیابی می‌توان به موارد زیر اشاره

سیستم‌های مربوط به نظارت، می‌توانند دسترسی‌های غیرمجاز به سیستم‌های کامپیوتری و حساب‌های مشتری را تشخیص دهند.

این روش، حداکثر ظرفیت و بازده سایت را به ازای هر کاربر و یا به ازای هر دسترسی کاهش می‌دهند: ساختار ظاهری سایت بسیار راحت است و عناصری مانند فریم‌ها، عکس‌های حجیم و محتوایی را که خارج از سایت اجرا می‌شوند، حذف می‌کنند. سایر تکنیک‌ها، مثل انتقال حجم کاری سرویس‌دهنده (انتقال پردازش‌ها از سرویس‌دهنده به سمت مشتری) و زمانبندی کردن تراکنش‌ها بر اساس مواقعی که سرویس‌دهنده در دسترس است نیز می‌تواند به وب‌سایت‌ها کمک کند تا تغییرات ایجاد شده در حجم کار سرویس‌دهنده را اداره کنند. بانک‌ها می‌توانند از هر یک از این روش‌ها یا ترکیبی از این روش‌ها جهت سرویس‌دهی به تعداد متغیر مشتریان بالقوه سایتشان استفاده کنند.

۴-۲-۴) سازگاری: ظاهر و عملکرد مناسب و هماهنگ یک سایت بانکداری اینترنتی هم از ضروریات موفقیت می‌باشد. وجود مشکلات و ناهماهنگی در سایت، از عملکرد صحیح آن جلوگیری می‌کند و در نتیجه، رضایت مشتریان و اعتماد به وب سایت مورد نظر را کاهش می‌دهد[۸].

وقتی که یک وب سایت بانکداری اینترنتی تنها برای تعداد خاصی از مشتریان با مشخصات خاص طراحی شده باشد، مشکلات مربوط به هماهنگی و سازگاری بروز خواهد کرد. این مشکلات زمانی اتفاق می‌افتند که بینندگان از کاوشگرهایی (و یا نسخه‌های متفاوت کاوشگر) استفاده کنند که در طول طراحی تست نشده‌اند، یا زمانی که برای اجرای وب‌سایت‌ها باید نرم‌افزارهایی به روی کامپیوتر مشتری نصب شود. بنابراین، وب‌سایت‌ها به صورت کلی باید توسط مجموعه مختلفی از نرم‌افزارها و سخت‌افزارها مورد بررسی قرار گیرند تا بتوانند قبول برای مشتری قابل قبول باشند، مشکلاتشان را کاهش‌دهند و به ایجاد فضای اعتماد کمک کنند.

۴-۳) روش‌های پرداخت: روش‌های متفاوتی برای پرداخت روی اینترنت وجود دارد. به صورت کلی، می‌توان آنها را به دو دسته Online (مثل Debit Cart) و Offline (مثل کارت اعتباری و چک اعتباری) تقسیم‌بندی کرد. به دلیل درگیر بودن طرف‌های متعدد در پرداخت اینترنتی، امکان استراق سمع افراد غیر مجاز حین انجام دستور پرداخت و احتمال حمله هکرها به سیستم‌های پرداخت و انجام فعالیت‌های کلاهبرداری و دزدی و یا از کار انداختن سیستم‌های پرداخت همواره وجود دارد. دسترسی آنلاین به سرور حق دسترسی بانک، استفاده از پروتکل‌های امنیتی رمزگذاری و احراز هویت، امضا و پاکت‌های دیجیتالی به هنگام ارسال دستورهای پرداخت، برای جلوگیری از هرگونه کلاهبرداری و پرداخت غیرمجاز ضرورت دارند. در سیستم‌های Offline به علت عدم دسترسی آنلاین به سرور حق دسترسی، احتمالات تقلب و کلاهبرداری بسیار افزایش می‌یابد.

البته در سیستم‌های پرداخت الکترونیکی مشکلاتی مانند احتمال کپی‌کردن اسناد مالی دیجیتالی، احتمال ایجاد امضای دیجیتالی جعلی و یا الحاق اطلاعات هویتی شخص پرداخت‌کننده به تراکنش مالی نیز وجود دارد. علیرغم چنین زیان‌هایی که شامل حال مشتریان و بانک‌ها می‌شود، وجود روش‌های پرداخت متعدد بر روی وب، انعطاف‌پذیری و امکان انتخاب‌های متعدد امنیتی و محرمانگی برای مشتریان

توابع درهم ساز (Hash Function)، کارت هوشمند، امضای دیجیتالی، گواهی‌های دیجیتالی و سیستم‌های ثبت وقایع، از جمله تکنیک‌های ایجاد انکار ناپذیری می‌باشند.

کرد: پیگیری تعداد مشتریانی که جهت دستیابی به کلمه و رمز عبور، کلاهبرداری را گزارش می‌کنند؛ تعداد کلیک‌ها بر روی لینک‌های مربوط به امنیت اطلاعات در وب‌سایت؛ و مقدار پولی که در اثر سرقت هویت از دست می‌رود [۱۸].

نتیجه گیری

در این مقاله، راجع به بانکداری اینترنتی به عنوان ابزاری برای انجام تراکنش مالی مشتریان از طریق وب‌سایت بر روی اینترنت بحث شده است. قبل، بعد و در طول تراکنش‌های بانکداری اینترنتی، مشتریان به خاطر ماهیت تراکنشی که انجام می‌دهند، با مخاطرات زیادی روبرو هستند. این ریسک‌ها به ریسک‌های مربوط به تکنولوژی و ریسک‌های تجاری تقسیم‌بندی می‌شوند. ما همچنین موارد کلیدی را که مشتریان و بانک‌ها برای ایجاد اعتماد بر روی سایت‌های بانکداری اینترنتی در مدنظر دارند، بیان کردیم: تراکنش‌های بین بانک و مشتری، تکنولوژی، روش‌های پرداخت، شرح کامل فعالیت بانک‌ها به مشتری، خوش نامی و آگاه‌سازی مشتریان. ما در مورد هر کدام از آنها فاکتورهای متعددی را مطرح کردیم و چگونگی تأثیر اعتماد مشتریان را بررسی نمودیم.

این مساله مهمی است که مشتریان بتوانند به تمام عناصر ایجاد اعتماد بحث شده در این مقاله دسترسی داشته باشند و همچنین همه فاکتورهایی که در ایجاد اعتماد بلندمدت و نخستین آنها تأثیر دارند، در نظر گرفته شوند. به علاوه، باید الگوهای مخصوص برای استفاده از چنین عناصری توسط افرادی با پیش زمینه یکسان یا متفاوت و یا برای وب‌سایت‌هایی با خصوصیات معمول مشخص شناسایی شوند.

علاوه بر این، می‌توان مجموعه‌ای از راهبردهای مفهومی و یا ابزارهایی برای ایجاد اعتماد در وب‌سایت‌های بانکداری اینترنتی را ایجاد نمود شوند تا طراحان وب با استفاده از این راهبردها، سایت‌های بانکداری اینترنتی مناسبی را طراحی کنند و پرسشنامه‌هایی را نیز جهت ارزیابی سطح اعتماد بازدیدکنندگان سایت بانکداری اینترنتی ایجاد نمایند.

وجود زیرساخت‌های کلید عمومی (PKI) و مراکز اعتماد (CA) در ایجاد گواهی‌های الکترونیکی (به عنوان ابزاری جهت تولید امضای دیجیتالی و مکانیسم‌های رمزنگاری متقارن و نامتقارن) از مهمترین عناصر ایجاد اعتماد در بانکداری اینترنتی می‌باشند. علاوه بر نقش CA در ایجاد زیرساخت‌های امنیتی اعتماد، وجود CA در کشور جهت اتصال بانک‌های داخلی به سیستم بانکداری الکترونیکی جهانی ضرورت دارد. بنابراین، راه‌اندازی زیرساخت‌های کلید عمومی (PKI) و مراکز اعتماد (CA) مهمترین قدم در راه ایجاد یک سیستم بانکداری اینترنتی جهانی و قابل اعتماد می‌باشند.

ظاهر و عمکرد مناسب و هماهنگ یک سایت بانکداری اینترنتی، از ضرورت‌های موفقیت است.

توجه:
منابع و مآخذ این مقاله در دفتر مجله موجود است و علاقمندان می‌توانند از آن استفاده کنند.