بانکداری

مدلسازی اعتماد در بانکداری اینترنتی

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

چکیده

از آنجایی که موفقیت بانکداری اینترنتی اساسا به مشتریان آن وابسته است، لذا می‌توان اعتماد مشتری را از مسایل اساسی در رشد و توسعه بانکداری اینترنتی به حساب آورد. در این مقاله، در مورد مسایل حیاتی موثر بر اعتماد مشتریان بر روی وب سایت های بانکداری اینترنتی، آنالیز گردش اطلاعات در بانکداری اینترنتی جهت تشخیص تهدیدات و ریسک‌های موجود در آن، ریسک‌های تکنیکی و غیرتکنیکی، توسعه و ایجاد مدل اعتماد (Trust Model) جهت مینیمم کردن ریسک‌های موجود و بهبود اعتماد مشتریان نسبت به این روش نوین بانکداری، بحث خواهد شد.

کلمات کلیدی:
مدل اعتماد، اعتماد، بانکداری اینترنتی

اعتماد مشتری، یکی از مسایل اساسی در رشد و توسعه بانکداری اینترنتی است.

مقدمه

برای انجام هر نوع تراکنش بانکی بر روی اینترنت، لازم است که کاربران مقداری از اطلاعات شخصی خود مانند نشانی، شماره تلفن، ایمیل و اطلاعات مربوط به کارت اعتباری خود را بر روی اینترنت وارد کنند. به علت گمنامی ذاتی موجود در بیشتر وب سایت‌ها و فقدان شناخت و تعامل کافی با مردم، بیشتر مردم نسبت به فاش شدن اطلاعات شخصی شان که از طریق اینترنت در اختیار بانک‌ها قرار داده‌اند، ابراز نگرانی می‌کنند. بیشتر آنها احساس می‌کنند که نمی‌توانند هیچ کنترلی بر روی عملکرد بانک‌ها نسبت به این اطلاعات داشته باشند و بانک‌ها می‌توانند به راحتی و به صورت غیرمجاز آن اطلاعات را در اختیار شرکت‌های ثالث قرار دهند. علاوه بر این، همیشه این ریسک وجود دارد که هکرها اطلاعات را در زمان انتقال و یا از روی سرویس دهنده بانک‌ها سرقت کنند. به دلیل حساسیت‌های موجود در اطلاعات مالی، تمام این مسایل باعث کاهش اعتماد مشتریان بانک‌ها در بانکداری اینترنتی می‌شوند.

بنابراین، کمبود اعتماد نسبت به امنیت و محرمانگی تراکنش‌های بانکی از طریق اینترنت، یکی از موانع مهم در راه استفاده گسترده مردم از بانکداری اینترنتی بشمار می رود. از آنجا که موفقیت و سود بانکداری اینترنتی اساسا به جذب مشتریان جدید و حفظ مشتریان فعلی وابسته است، لذا اعتماد مشتریان، از مسایل اساسی در بقای بانکداری اینترنتی است. در نتیجه، ایجاد و نگهداری اعتماد (Trust) در بانکداری اینترنتی، امری بسیار مهم می‌باشد. برای تحقق این امر مهم، فرموله کردن مدلی به نام مدل اعتماد (Trust Model) به عنوان قسمتی از متدلوژی امنیت، و آنالیز و بررسی ریسک‌ها و تهدیدات موجود در سیستم بانکداری اینترنتی و کاهش تهدیدات و ریسک‌های شناسایی شده جهت ایجاد اعتماد را دنبال می‌کنیم.

این مقاله شامل تعریف Trust و انواع آن، نگاهی بر بانکداری اینترنتی، ایجاد و نگهداری مدل اعتماد در بانکداری اینترنتی و نهایتا نتیجه گیری می‌باشد.

اعتماد و بانکداری اینترنتی

موجودیت‌های مختلفی، از جمله بانک‌ها، مشتریان و طرف‌های ثالث، در انجام تراکنش‌های بانکی از طریق اینترنت دخالت دارند. در اینجا نقش هر یک را در یک مدل ساده بانکداری اینترنتی تشریح می‌کنیم و در مورد چگونگی ایجاد اعتماد در این زمینه، که پایه آن وب است، بحث خواهیم کرد.

۱-نگاهی به بانکداری اینترنتی: استفاده از سرعت و سادگی منحصر به فرد اینترنت در انجام تراکنش‌های بانکی را اصطلاحا بانکداری اینترنتی می گویند. در این راستا مشتریان، سرویس مورد نیاز خود- یا هر گونه تراکنش با بانک- را از طریق وب سایت بر روی اینترنت انجام می دهند. از سوی دیگر، بانک‌ها نیز سرویس‌های خود را بر روی وب سایت قرار می‌دهند. شرکت‌های ثالث نیز با فراهم

مدل اعتماد، قسمتی از متدولوژی ایجاد امنیت از طریق شناسایی و کاهش ریسک‌هاست.

سازی تکنولوژی سیستم‌های بانکداری تحت وب، در بانکداری اینترنتی سهیم می‌باشند.

برای انجام عملیات بانکی تحت وب، لازم است مشتریان اطلاعاتی در مورد بانک مربوطه، سرویس‌های مورد نیاز و مشخصات آن‌ها داشته باشند. بانک‌ها نیز همچنان‌که از فعالیت‌ها و استراتژی های تجاری بهره می‌برند، از زیرساخت‌های تکنولوژی جهت پشتیبانی از وب سایت‌هایشان استفاده می‌کنند(مانند سرورها، سیستم‌های اطلاعاتی، پایگاه داده، سیستم‌های پرداخت و مکانیسم‌های امنیت و محرمانگی). برخی از خدمات پایه مثل نمایش اطلاعات بانکی، پروسه انجام تراکنش‌های بانکی و پشتیبانی از مشتریان (قبل، در طول و بعد از انجام فعالیت بانکی) باید از طریق وب سایت‌ها فراهم شوند.

مدل‌های مختلفی از بانکداری اینترنتی وجود دارند[۱۰]:

* مدل‌های اطلاعاتی (Informational) که تنها اطلاعاتی را در مورد خدمات بانکی ارایه می دهند که به صورت سنتی در حال انجام است. این نوع بانکداری اینترنتی، دارای ریسک کمتری است.

* مدل‌های اطلاع رسانی (Communicative) که اطلاعات مربوط به حساب‌های بانکی را ارایه می‌کنند، و در صورت امکان عمل به روز رسانی اطلاعات ایستا مثل نشانی مشتریان را نیز انجام می‌دهند. در این نوع بانکداری اینترنتی، زمانی که دسترسی به سیستم اصلی بانک مجاز باشد، ریسک مساله ساز خواهد شد.

* مدل‌های تراکنشی (Transactional) که به مشتریان اجازه اجرای تراکنش‌های مالی را می‌دهند و بیشترین ریسک را متحمل می‌شوند. بدیهی است که بعضی از مدل‌های تراکنشی ریسک بیشتری دارند، مثل وقتی که مشتری هرگز شعبه‌ای را در راستای روابط خود ندیده و در عین حال، می‌خواهد تمام تراکنش‌های خود را از راه دور انجام دهد.

۲-اعتماد در بانکداری اینترنتی: اعتماد بسته به دامنه کاربرد آن، دارای تعاریف مختلفی است، اما صورت عمومی اعتماد را این گونه تعریف می‌کنند: با اطمینان تکیه کردن بر روی شخصیت، توانایی، قدرت، حقیقت و راستی هر فرد یا هر چیزی، و یا اطمینان و اعتماد به مشخصات و ویژگی‌های یک شیئی یا فرد و یا حقیقت و حالت آن. بعضی نگرش‌ها اعتماد را به عنوان یک پاسخ درونی و شخصی می‌پندارند و عده‌ای دیگر آن را تنها به عنوان یک ارزیابی منطقی از قابلیت اطمینان فرض می‌کنند.

براساس ۵۰۹، X-TTU T، بخش ۳۰۳۰۵۴، اعتماد (Trust) این گونه تعریف می‌شود: به صورت معمول زمانی می‌توان گفت یک موجودیت به موجودیت دوم اعتماد دارد که موجودیت نخست فرض کند که رفتار موجودیت دوم مطابق با انتظار موجودیت فرد نخست است[۱۹].

به طور کلی، اعتماد به عنوان یک فاکتور ضروری در معرفی یک محصول یا سرویس جدید در حیطه تکنولوژی اطلاعات (مثل بانکداری اینترنتی) مطرح می‌باشد[۱۱].

اعتماد در بانکداری اینترنتی انتظاراتی است که یک سرویس یا محصول بانکداری اینترنتی باید برآورده کند یا تعهداتی است که باید انجام دهد. در این تعریف، انتظارات کاربران بر پایه نکات بسیاری استوار است مثل:

* تجربیاتی از خدمات و برنامه های قبلی و سنتی بانک

کاربران بانکداری اینترنتی، برای شهرت و خوشنامی ارایه کنندگان خدمات بانکداری بر روی اینترنت اهمیت زیادی قایل هستند.

در برابر تجربیات نسبت به بانکداری اینترنتی .

* تجربیاتی از تکنولوژی جدید بانکداری اینترنتی.

* شهرت و خوشنامی ارایه کنندگان خدمات بانکداری بر روی اینترنت.

* دانش کاربر نسبت به بانکداری اینترنتی.

* اعتماد یا عدم اعتماد نسبت به عامل و نماینده‌ای که خدمات بانکداری اینترنتی را ارایه می‌دهد.

بدیهی است که سطح اعتماد افراد، با تغییر در انتظاراتشان تغییر می‌کند.

مدل اعتماد هم فرایندی است برای تشخیص تهدیدات و ریسک‌ها براساس آنالیز گردش اطلاعات در هر سیستم اطلاعاتی، که نتیجتا مکانیسم‌هایی را که برای پاسخ به یک تهدید خاص لازم و ضروری می باشند، شناسایی می‌کند[۱۹].

بنابراین، هدف از مدل اعتماد، پاسخ به یک دسته مشخص از تهدیدها و آسیب پذیری‌هایی است که از طریق نمودارهای آنالیز گردش اطلاعات موجود در هر سیستمی، مثل سیستم بانکداری اینترنتی، بدست می‌آید. مدلسازی سطح اعتماد در هر سازمان و موقعیتی، با سازمان و موقعیت دیگر فرق دارد. بنابراین، عناصر موجود در مدل اعتماد برای هر موقعیت، راه حل مناسبی برای همه موقعیت‌ها نمی‌باشند.

مساله اساسی در تعریف اعتماد و پارامترهای آن، اساسا به احراز هویت و تصدیق اصالت از طریق کلید عمومی (Public Key) توجه دارد[۱۲].

مدل اعتماد و پارامترهای مربوط به سیستم‌های Public Key Infrastructure به احراز هویت و تصدیق اصالت بین فروشنده و گیرنده، صحت پیام و محرمانگی پیام اشاره دارند. اینها همگی جنبه‌هایی از یک مدل امنیت (Security Model) می‌باشند. به همین دلیل، گاهی اوقات مدل امنیت و مدل اعتماد به جای یکدیکر بکار برده می‌شوند. از دید کاربران، امنیت اعتماد به این مساله است که تکنولوژی اطلاعات و کامپیوتر قادر باشند اعمال درخواستی آنها را به درستی انجام دهند. اما از دید کاربران، فاکتورهایی غیر از امنیت نیز در ایجاد اعتماد مهم هستند، از جمله این فاکتورها، قابلیت استفاده (به درد بخوری)، قابلیت اطمینان، در دسترس بودن، محرمانگی و امن بودن می‌باشند که جنبه روان شناسی دارند[۱۱]. بنابراین، به طور کلی، در توسعه یک مدل اعتماد مناسب، هم جنبه روان شناسی و هم جنبه فنی و تکنیکی ضروری می‌باشند. علاوه بر این، مدل اعتماد باید توسط کاربران مختلف با ویژگی های متفاوت قابل استفاده باشد.

مدل اعتماد همچنین ارتباط بین بررسی صحت چیزی (Verification) و اعتماد نسبت به آن (Trust) را نیز بازبینی خواهد کرد. مثال‌های مختلف این ارتباط شامل اعتماد پنهان (اعتماد بدون بررسی صحت)، اعتماد همراه با بررسی صحت، اعتماد بر اساس تجربه قبلی، اعتماد بر اساس دانش و اعتماد بین مدیران و نمایندگان (انتشار

اعتماد) می‌باشد[۱۱].

مکانیسم‌های رمز نگاری مثل امضاهای دیجیتالی، مکانیسم تصدیق اصالت، احراز هویت، صحت داده و محرمانگی نیز از جمله نیازمندی‌های مدل اعتماد در بانکداری اینترنتی بشمار می آیند.

آنالیز گردش اطلاعات در بانکداری اینترنتی و ریسک‌های موجود

فرض کنید که مشتری قصد دارد تراز حساب و عملیات بانکی خود را از طریق اینترنت به صورت آنلاین انجام دهد و بانک نیز مشخصات اعتباری ، مانند کلمه عبور و نام کاربری آنها را ایجاد کرده است. بنابراین، روند گردش کار به صورت زیر خواهد بود[۱۹]:

* مشتریان یک جلسه یا Session با سرویس دهنده بانک خواهند داشت. پروتکلی که این جلسه را کنترل می‌کند، SSL می باشد.

* کانال ارتباطی سرویس دهنده SSL ساخته می‌شود که تمام مراحل بعدی را پوشش می‌دهد.

* مشتری اطلاعات لازم مانند نام، شماره حساب و PIN را در صفحه ورود به سیستم وارد می‌کند.

* سرویس دهنده تصدیق اصالت و احراز هویت (Authentication Server) این مشخصات اعتباری کاربر را تایید می‌کند.

* سرویس دهنده وب، صفحه خوش آمدگویی و منویی

ریسک از بین رفتن امنیت در بانکداری اینترنتی، بسیار زیاد است، زیرا در این سیستم، داده‌های حساس مالی در حال نگهداری و رد و بدل شدن می باشند.

از تمام مواردی را که کاربر می‌تواند انتخاب کند و انجام دهد، نمایش می‌دهد.

* موارد انتخاب شده، به صورت یک درخواست به سمت سرویس دهنده برنامه کاربردی بانکداری فرستاده می‌شوند.

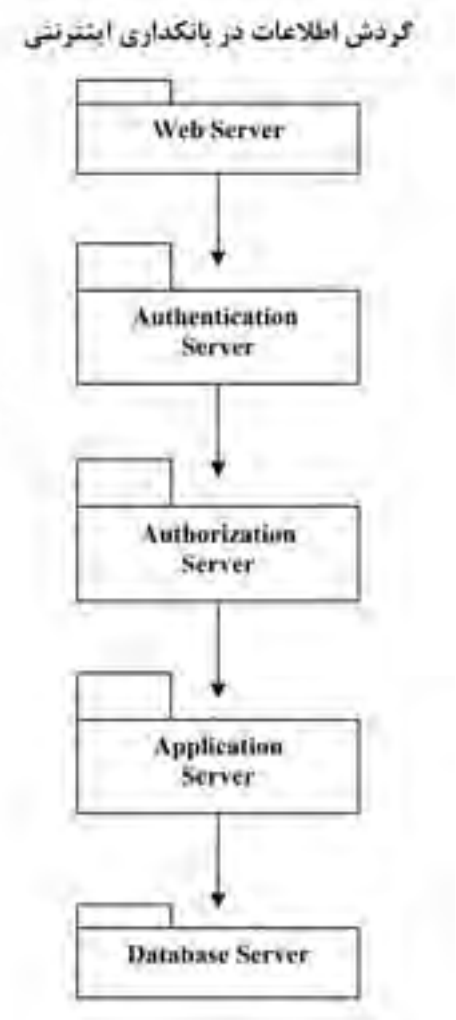
* سرویس دهنده برنامه بانکداری اینترنتی، یک درخواست را به سمت سرویس دهنده مربوط به کنترل حق دسترسی، جهت بررسی حق دسترسی گزینه‌های انتخاب شده می‌فرستد.

* سرویس دهنده کنترل حق دسترسی، بر اساس قوانین تعریف شده موجود، یک پاسخ به سرویس دهنده برنامه کاربردی ارسال می‌کند، مثلا اجازه دسترسی دارد.

* سرویس دهنده برنامه کاربردی بانکداری، از سرویس دهنده پایگاه داده می‌خواهد تا کلیه رکوردهای مربوط به درخواست آن حساب خاص را بدست آورد.

* سرویس دهنده پایگاه داده، رکوردها را به سمت سرویس دهنده برنامه کاربردی برمی‌گرداند.

* سرویس دهنده برنامه کاربردی، اطلاعات را به فرمت دلخواه درآورده و آن را به سمت سرویس دهنده وب جهت نمایش به مشتری ارسال می‌کند(شکل زیر).



توجه کنید که SSL تمام این جریان داده‌ها، از مشتری به سرویس دهنده و از سرویس دهنده به سمت مشتری را رمز گذاری می‌کند.

در این تراکنش، دو نوع داده پردازش می‌شوند:

۱)اطلاعات مربوط به احراز هویت و تصدیق اصالت مشتری (نام، شماره حساب و PIN).

۲)اطلاعات مربوط به حساب مشتری (تراز حساب).

یک آنالیز کامل، نیازمند بررسی نوع داده پردازش شده در هر نقطه اعتماد (Trust Point)، شناسایی انواع تهدیداتی که آن نقاط را تحت تاثیر قرار می‌دهند و راهکارهای مقابله با آنها است.

برای تحقق این هدف، ابتدا سرویس دهنده‌های مختلف را شناسایی می‌کنیم که شامل:

Data base server, Application server, Web service server, Authentication server, SSL server, Authorization server می‌باشند. سپس کانال‌های ارتباط و نقاط اعتماد را که گردش اطلاعات در راستای آنها صورت می گیرد، شناسایی می‌کنیم. هر کدام از نقاط اعتماد، یک نقطه مستعد برای حمله نیز می‌باشند، و از دست رفتن امنیت در هر یک از آنها، باعث وارد آمدن آسیب زیادی می‌شود. شایان ذکر است که ریسک از بین رفتن

مدل سازی سطح اعتماد هر سازمان و موقعیتی، با سازمان و موقعیت دیگر فرق دارد.

امنیت در بانکداری اینترنتی بسیار زیاد است، زیرا داده‌های حساس مالی در حال نگهداری و رد و بدل شدن می‌باشند.

پروسه برآورد ریسک باید شامل مراحل زیر باشد:

* تشخیص تمام تراکنش‌ها و سطوح دسترسی مرتبط با برنامه و سرویس‌های تحت وب مشتری.

* تشخیص و دسترسی به تکنیک‌های کاهش ریسک، شامل متدهای تصدیق اصالت و احراز هویت، که برای هر نوع تراکنش و سطوح دسترسی بکار گرفته می‌شود.

* وجود توانایی لازم برای قضاوت در مورد کارایی تکنیک‌های موجود، کاهش ریسک و تغییر فاکتورهای ریسک برای هر نوع تراکنش و سطوح دسترسی.

ریسک‌ها و تهدیداتی که از این گردش اطلاعات استخراج می‌شوند، عبارتند از:

* دسترسی افرادی به غیر از صاحبان حساب (افراد غیرمجاز) به اطلاعات.

* دیده شدن اطلاعاتی بیشتر از حد توسط صاحبان حساب.

* توانایی انجام تراکنش‌ها و اعمال غیرمجاز توسط صاحبان حساب یا دیگران.

* انجام تراکنشی توسط صاحب حساب و انکار بعدی او، یا انکار بانک‌ها از انجام چنین تراکنشی.

* حملات ناشی از ویروس‌ها، و رم‌ها و سایر کدهای مخرب.

* دزدیده شدن، تغییر یا انجام هرگونه پردازش غیرمجاز بر روی رکوردهای اطلاعاتی در جریان تبادل اطلاعات و یا از روی سرویس دهنده بانک‌های اطلاعاتی توسط افراد غیر مجاز.

* دزدیده شدن کلمه و رمز عبور در جریان تبادل اطلاعات و یا از روی سرویس دهنده‌ها توسط افراد غیر مجاز (با تدارک دیدن حملات مختلف) و تکرار حملات و انجام تراکنش‌های غیرمجاز مالی و دیگر فعالیت‌های غیرمجاز.

* حمله DOS به هر یک از سرورهای فوق، و ارسال درخواست‌های بیش از حد به سرویس دهنده‌های مورد نظر، که در کار آنها اختلال ایجاد کرده و باعث می‌شود که نتوانند به درخواست‌های مجاز پاسخ دهند.

تمام موارد ذکر شده از جنبه‌های تکنیکی تهدیدات و ریسک‌های وارد بر بانکداری اینترنتی می‌باشند که از آنالیز گردش اطلاعات استخراج شده‌اند. علاوه بر آنها، ریسک‌های دیگری نیز از جانب خود بانک‌ها، مشتریان را تهدید می‌کنند که شامل موارد زیر می‌باشند[۱۰]:

* سوء استفاده از اطلاعات شخصی مشتریان: اطلاعات مشتریان زمانی که بر روی وب سایت وارد شد، به راحتی قابل ویرایش است. مشتریان بیشتر اوقات مجبورند اطلاعاتی مانند نشانی، سن، جنس و حتی بعضی مواقع سطوح درآمد خود را در وب سایت‌های مربوط به بانکداری اینترنتی وارد کنند. این اطلاعات به راحتی می‌توانند به صورت غیرقانونی مورد سوء استفاده قرار گیرند و یا ممکن است به شرکت‌های ثالث غیرمجاز داده شوند.

* عدم تکمیل صحیح تراکنش‌های بانکی توسط بانک‌ها: زمانی که بانک‌ها تراکنش‌های آنلاین بانکی را آن چنان که متعهد شده‌اند، انجام ندهند و هیچ گونه پشتیبانی از خدمات خود نداشته باشند، مثل نقص در ارایه ۲۴ ساعته و هفت روزه هفته خدمات بانکی، انکار بانک‌ها از انجام تراکنش توسط مشتری، خطا، کوتاهی و ناتوانی در انجام تراکنش با مشتری و یا وجود نقص در نرم افزارها و برنامه‌های بانکداری اینترنتی که همگی موجب کاهش خوشنامی بانک‌ها و در نتیجه، سلب اعتماد مشتریان می‌شوند.

* تجاوز به نظم، قوانین و استانداردهای اخلاقی توسط بانک‌ها: این ریسک باعث کاهش شهرت، خوشنامی ، درآمد، شانس تجاری و اعتماد مشتریان بانک ها می‌شود. بنابراین، لازم است که بانک‌ها، قوانین موجود و حاکم بر بانکداری اینترنتی را به خوبی تفسیر و درک کنند و خود را با سایر بانک‌ها و شعب هماهنگ و سازگار سازند. این ریسک زمانی واقع می‌شود که تراکنش بانک‌ها و مشتریان در بیشتر از یک کشور اتفاق می افتد و اختلاف در قوانین و ملزومات مالی هم موجب ایجاد ریسک می شوند.

* ریسک تبادلات ارزی: بانکداری اینترنتی باعث می‌شود که سایر کشورها با واحد پولی خودشان بتوانند با بانک‌ها به صورت آنلاین تراکنش کنند. این امر خود باعث سادگی و کاهش هزینه مبادلات می‌شود. البته اگر مشتریان مجبور باشند با واحد پولی غیر از واحد پولی خود تبادلات مالی گسترده‌ای را انجام دهند، این نوع ریسک افزایش می‌یابد.

ادامه دارد

کاربران حق دارند که از فناوری‌های نوین دنیای دیجیتال برخوردار شوند.

توضیح: فهرست منابع این مقاله، در پایان آخرین بخش چاپ خواهد شد.