بهبود امنیت بانکداری اینترنتی با استفاده از احراز هویت متفاوت براساس توصیف ریسک پذیری

چکیده

امنیت آنلاین یک چالش برای اطمینان از تراکنش امن بر روی اینترنت است. احراز هویت کاربر، یک فرایند انسان محور است، که به‌عنوان پایه‌ی امنیت کامپیوتر در نظر گرفته می‌شود و از این رو دسترسی به خدمات بانکداری آنلاین را تضمین می‌کند. افزایش استفاده از تکنولوژی برای به اجرا درآوردن اقدامات اضافی، توانایی بهبود کیفیت احراز هویت و امنیت آنلاین را می‌طلبد. هدف از این مقاله تعیین این است که اگر عواملی برای احراز هویت کاربران وجود دارد، می‌تواند برای کاربران بانکداری اینترنتی نیز استفاده شود، برای مثال، شناسایی احراز هویت پس از طبقه‌بندی ایمنی آن‌ها براساس مرورگری که آنها استفاده می‌کنند، بررسی مبتنی بر وب برای تعیین برداشت مشتریان آنلاین از مهارت‌های خود و ایجاد کلمات عبور و شیوه‌های مدیریت و ضبط اطلاعات دموگرافیک همانند مرورگرهای استفاده شده، طراحی شده است. بعد از استفاده از یک ساختار برای عملکرد رمز عبور، که از تحقیقات قبلی بر روی مجموعه داده‌های یکسان بدست آمده است، مرورگر مورد استفاده با به کاربردن رمز عبور ضعیف مقایسه می‌شود. براساس نتایج بدست آمده، یک مورد می‌تواند توسط روش‌های تأیید هویت مختلف برای مشتریان و براساس مرورگر انتخابی آنان برای اطمینان در محیط آنلاین امن‌تر ایجاد شود.

کلیدواژه‌ها: بانکداری آنلاین، احراز هویت کاربر، احراز هویت متمایز، توصیف ریسک

1. معرفی

رشد فوق العاده بانکداری آنلاین راه این مسیر را به وجود آورده است که مشتریان با ارائه‌دهندگان خدمات مالی تعامل برقرار کنند. تعامل اکثریت مشتریان با ارائه‌دهندگان خدمات به‌صورت آنلاین و از طریق مرورگر مورد نظر خود رخ می‌دهد و به طور فزاینده‌ای به سمت خدمات تلفن‌همراه در حال پیشرفت است. احراز هویت کاربر، پایه و اساس امنیت کامپیوتر (Conklin، Dietrich و Walz، 2004: 1) و کلمات عبور است، در ترکیب با اقدامات دیگر، احراز هویت کاربران بانکداری آنلاین بسیار حیاتی است.

کاربران کامپیوتر یک پیوند ضعیفی با امنیت آنلاین دارند زیرا شیوه‌های به‌کارگیری رمز عبور اثر مستقیمی بر سطح امنیت یک سیستم دارد (Gehringer، 2002 :369). نه تنها انتخاب و مدیریت رمزهای عبور ممکن است رمز عبور را در معرض سوءاستفاده احتمالی قرار دهد (Furnell و، 2005: 10). بلکه اگر کاربران رمزهای عبور خود را به درستی انتخاب و مدیریت نکنند اکثر سیستم‌های امنیتی پیشرفته به خطر می‌افتند (Tam، Glassman و Vandenwauver، 2010 :233). علیرغم وجود مشکلات مربوط به امنیت رمز عبور، کلمه عبور به‌عنوان ابزاری برای شناسایی کاربران، چه به تنهایی یا ترکیبی، رایج‌ترین روش احراز هویت است (Furnell و، 2005: 9 و 11).

فن‌آوری پشتیبانی سیستم‌های جدید احراز هویت مانند بیومتریک و پین یک بار مصرف در حال حاضر بسیار محبوب هستند (Tam و همکارانش 2010: 233) و به امنیت محیط آنلاین کمک می‌کنند. بااین حال، استفاده از این تکنولوژی به صورت یکنواخت به همه کاربران اعمال شده است. این یکی از ویژگی‌های کاربران است که برای ایجاد احراز هویت های متمایز استفاده نمی‌شود. همه کاربران، صرف نظر از هر گونه دانش اضافی که ممکن است شناخته شده باشد، به هنگام احراز هویت، به‌صورت یکسان با انها رفتار می‌شود.

2. بانکداری آنلاین

همانگونه که کاربر بانکداری آنلاین مسائل امنیتی مربوط به محرمانه بودن را افزایش می‌دهد، صداقت، و حفظ حریم خصوصی نیز تبدیل به نگرانی بانک و مشتریان می‌شود. بانک ها مزایایی مانند افزایش بهره‌وری و مشتری از طریق این

رسانه جدید را مهیا می‌کنند. با وجود حضور در حال رشد خدمات بانکداری آنلاین، نگرانی‌های امنیتی و حفظ حریم خصوصی و ترس هنوز هم قبل از هر چیز دیگری در ذهن کاربران وجود دارد و با آن مواجه هستند.

تقریبا به ناچار، رشد نمایی بانکداری اینترنتی متناظر با افزایش سریع و دردسترس تقلب در این حوزه است. بنا به منابع مالی در خطر، مجرمان اینترنتی از منابع بیشتر و افزایش قابلیت‌های فن‌آوری برای انجام کلاهبرداری‌های آنلاین استفاده می‌کنند. بنا به این که معاملات بانکداری از مکان‌های فیزیکی با خزانه‌های محافظت شده به مشتریانی با دارایی‌های آنلاین نقل مکان کردند، مجرمان اینترنتی نیز پا به عرصه گذاشتند (Rice، 2012: 441).

احراز هویت کاربر، برای خدمات بانکداری آنلاین، چیزهایی را که یک کاربر می‌داند یا دارد و یا چیزی که کاربر انجام می‌دهد به کار می‌گیرد (به جدول 1 اشاره شده است). بنا به افزایش خطرات گوناگون در محیط‌های اینترنتی، روش‌های تأیید هویت کاربر متنوع‌تر شده و در بانکداری آنلاین بیشتر از سایر روش‌های ترکیبی دو یا بیشتر عوامل به کار گرفته می‌شوند.

3. به کارگیری فن‌آوری

به خوبی ثبت شده است که روش‌های شناسایی سنتی شخص، مانند کلمه عبور، از اشکالات زیادی رنج می‌برد و قادر به برآوردن امنیت در جامعه اطلاعاتی بسیار متصل نیستند. در نتیجه فن‌آوری‌های مختلفی برای احراز هویت آنلاین توسعه و اجرا شده‌اند.

• بیومتریک‌ها اشاره به هویت فردی براساس صفات رفتاری یا فیزیولوژیکی خود فرد هستند. محدوده‌ی استفاده از ویژگی‌های فیزیکی از جمله voiceprints، اثرانگشت و تشخیص عنبیه چشم، به ویژگی‌های رفتاری از جمله راه رفتن و تشخیص دست خط فرد برمی‌گردد. بیومتریک‌ها ذاتا برای کپی کردن، به اشتراک‌گذاری، توزیع و جعل دشوار هستند و از همه مهمتر بنا به حضور فیزیکی فرد نمی‌توان آنها را فراموش یا از دست داد (Kaman، Swetha Akram و Varaprasad، 2013؛ Tassabehji و Kamala، 2012).

• علاوه براین احراز هویت یک روش تأیید هویت کاربر با استفاده از یک کانال جدای از تسهیل تراکنش‌ها به‌منظور بهبود امنیت آنلاین است (Fieg، 232007 :). بااستفاده از کانال ارتباطی ثانویه‌ای که باید برای همان کاربر منحصر به فرد باشد، سطح امنیت تا حد زیادی بهبود می‌یابد و به یک استاندارد در بانکداری آنلاین تبدیل می‌شود.

• کلمه عبور گرافیکی به‌عنوان جایگزین برای رمز عبور احراز هویت مبتنی بر متن ارائه شده است. Biddle، Chiasson و Van Orschot (2012) مروری جامع بر تحقیقات منتشر شده، پوشش هر دو قابلیت و جنبه‌های امنیتی و همچنین ارزیابی سیستم را ارائه کرده‌اند.

• پین یک بار مصرف (OTP) یک سیستم است که در آن پیام‌های متنی برای استفاده‌ی یک بار به‌منظور بررسی ورود به سیستم به تلفن‌همراه فرستاده می‌شود. این روش محبوب یک زیرمجموعه از روش‌های احراز هویت است. برخی از برنامه‌های جدیدتر PIN یک بار مصرف، یک گواهی دیجیتال بر روی تلفن کاربر جهت احراز هویت تراکنش‌های آتی است. سیستم به تمام شماره تلفن‌های تلفن همراه تکیه نمی‌کند بلکه بنا به گواهی دیجیتال واقعی بر روی گوشی عمل می‌کند (Wolf، 2011).

• سیستم کلید پویا یک تکنولوژی است که اطمینان حاصل می‌کند کاربر، پس از احراز هویت، در واقع احراز هویت کاربر به درستی صورت گرفته است (Pisani و Lorena، 2013). مزایای کلید پویا، اگر چه برای پیاده‌سازی پیچیده است و نیاز به پردازش فشرده‌ای دارد، اما از ماهیتی غیرسرزده با نظارت مستمر پس از احراز هویت برخوردار است.

در میان افزایش فشار برای محافظت از مشتریان آنلاین، برخی از بانک‌های جهانی بزرگ به سمت احراز هویت دو عاملی و چند کانالی پیش رفته‌اند. بااین حال، تمام اقدامات به‌طوریکنواخت به تمام کاربران، بدون در نظر گرفتن اطلاعاتی که ممکن است در نمونه احراز هویت، و یا حتی پس از احراز هویت کاربر و صفات مرتبط با کاربران شناخته شده باشد اعمال می‌شود. بحث پراهمیت در عملکرد رمز عبور ضعیف، به رسمیت شناختن رمز عبور مناسب سیستم‌های امنیتی شامل هر دو جنبه انسانی و تکنولوژیکی است (Brostoff و Sasse، 2002: 41). اقدامات فنی گنجانیده شده در سیستم‌های امنیتی کم ارزش خواهند بود اگر کاربران از اقدامات، خطرات یا نتایج مرتبط با ضعف رمز عبور اطلاعاتی نداشته باشند.

4. چالش کاربران

Conklin و همکارانش (2004: 5) به کاربر آموزش ندیده به‌عنوان یکی از ضعیف‌ترین لینک‌ها در یک سیستم امنیتی توجه دارند. درحالی‌که کاربران با رمز عبور خاص ممکن است در استفاده از رمز عبور مناسب بسیار ماهر عمل کنند، اقدامات امنیتی مناسب و دستورالعمل اغلب توسط کاربران، ناشناخته، بی‌توجه و یا توسط کاربران کامپیوترهای دیگر اجتناب می‌شوند. (Notoatmodjo و Thomborson، 2009 :71). با این حال، موسسات از همان روش احراز هویت برای همه کاربران استفاده می‌کنند. به عنوان مثال، ایجاد یک روش احراز هویت پیچیده مجهز به حداقل امنیت کاربر برای اطمینان از شکست احراز هویت امن به رغم دانش امنیت اینترنتی بسیار محدود، موانع ورودی غیرضروری را برای احراز هویت کاربران که به شیوه‌ای امن رفتار می‌کنند افزایش می‌دهد. سطح افتراق دانش و برنامه در میان کاربران تبدیل به یک نگرانی شده است، اما یک فرصت برای افزایش آنلاین ایمنی در موارد مورد نیاز است.

در اصل، تنها سه دسته احراز هویت وجود دارد که می‌تواند برای تضمین محیط آنلاین نشان داده شده در جدول 1 مورد استفاده قرار گیرد.

جدول 1: انواع احراز هویت

انواع احراز هویت	اعتبارسنجی	مثال‌ها
اثبات دانش	چیزی که کاربر می‌داند. دانش ضمنی یا دانش به اشتراک گذاشته شده توسط ارائه دهنده خدمات	کلمه عبور، PIN، شماره تلفن
اثبات	چیزی که کاربر در اختیار داد	کارتهای هوشمند، نشانه، دستگاه‌های سخت‌افزار، گواهینامه‌های دیجیتال
اثبات مشخصات	وسیله‌ای فیزیکی یا ویژگی رفتاری	اثر انگشت، الگوهای رگ مچ دست، اسکن شبکیه چشم، تشخیص صدا و صورت

Choubey و Choubey (2013) تعدادی از ویژگی‌های امنیتی استفاده شده توسط بانک‌های مختلف در سطح جهانی را بررسی کردند. اقدامات به کار گرفته شده از رمز عبور ساده تنها مربوط به سیستم‌هایی با ساختارهای پیچیده شامل یک OTP از طریق ایجاد سخت افزار خارجی است. جایی در بین سیستم‌ها که شامل اطلاعات اضافی براساس کلمات به یاد ماندنی و یا اطلاعات دیگر کاربران است.

با توجه به موسسات Choubey و Choubey که در معرفی لایه‌های بیشتر امنیت دستی دارند دسترسی و استفاده از اطلاعات مالی خود برای کاربران نهایی به دشواری بیشتری منجر شده است. علاوه بر این، گسترش ویژگی‌های امنیتی منجر به دشواری تست امنیت در بانک‌های مختلف و همچنین ایجاد زحمت و دردسر برای کاربران به هنگام رفتن به یک موسسه دیگر شده است. آنها حتی استدلال می‌کردند که منحنی یادگیری در ارتباط با انواع مختلف ویژگی‌های امنیتی بتواند تبدیل به یک تنگنا در تنوع بازار آینده شود (Choubey و Choubey، 2013 :202).

5. هزینه، راحتی و مسئله امنیت

مهمترین موضوع در امنیت آنلاین، انتخاب رمزهای عبور قوی است که به‌سختی قابل حدس زدن باشد (امن) اما هنوز هم رمزهای به یاد ماندنی، مناسب هستند (Conklin و همکاران 2004: 5). با این حال، هنگامی که با کلمه عبور کاربران به‌عنوان تجارت جهانی امنیت روبه‌رو می‌شویم (Tam و همکارانش 2010: 242)، یک درگیری بین راحتی به خاطر سپردن و امنیت کلمات عبور به وجود می‌آید (Weber، Guster، Safanov و Schmit، 2008: 46). بسته به اینکه امنیت و یا راحتی قبل از هر چیز برای کاربران نگرانی ایجاد کند، رمز عبور هم امن یا غیرامن خواهد بود.

Yan، Blackwell، Anderson و Grant (2004: 25) مشخص کردند که کاربران به ندرت کلمه عبوری که هم برای حدس زدن سخت باشد و هم به آسانی به خاطر سپرده شود انتخاب می‌کنند. عواملی که امنیت رمز عبور را افزایش می‌دهند افزایش تعداد سیستم محافظت از رمزعبور هستند که، طول عمر رمزعبور و ترکیب قواعد و محدودیت حافظه انسان را درنظر می‌گیرند (Chiasson و Biddle، 2007: 1؛ Yan و همکارانش 2004: 25؛ Furnell و، 2005: 10). این نتایج در کاربران موجب توسعه‌ی روش آنها در به خاطر سپاری کلمه عبور می‌شود. زمانی که انگیزه‌های امنیتی ثانویه به راحتی منجر به تعیین رمز عبور ضعیف می‌شوند، شامل استفاده از کلمات عبور کوتاه و ضعیف هستند که به خاطرسپاری، به اشتراک‌گذاری کلمات عبور، نوشتن کلمه عبور، استفاده مجدد از کلمه عبور و

عدم تغییر منظم کلمه عبور را آسان می‌کنند (Campbell، Kleeman و Ma، 2007: 3؛ Furnell و، 2005: 10؛ Notoatmodjo و Thomborson، 2009 :71).

متاسفانه قابلیت استفاده از فن‌آوری‌های امنیتی اغلب توسط طراحان نادیده گرفته می‌شود (Brostoff و Sasse، 2002 :41). Furnell و Brostoff و Phippen (2007: 416) بهبود قابلیت استفاده از ویژگی‌های امنیتی را که اغلب کاربران از آنها استفاده نمی کنند توصیه می‌کنند چرا که مشکلاتی برای یافتن، درک و استفاده از این ویژگی‌های امنیتی دارند. Inglesant و Sasse (2010) توصیه تاکید بر اصول واسط کامپیوتر انسان (HCI) برای افزایش امنیت رمز عبور دارند.

6. احراز هویت متفاوت

Furnell و (2007: 445) اظهار می‌دارد که یکی از دلایلی که بسیاری از کاربران کامپیوتر از شیوه‌های رمز عبور بی‌خطر استفاده نمی‌کنند این است که به دلیل فقدان دانش مناسب، هدایت و حمایت مطمئن نیستند. تا به امروز تمام موارد احراز هویت به‌طور یکنواخت به کاربران اعمال می‌شد. صرف نظر از هر گونه دانش شناخته شده‌ای در مورد رفتار آنلاین کاربران، (و سطوح امنیت) روش احراز هویت برای همه کاربران مورد نیاز است.

با توجه به پژوهش Ciampa، Mark و Enamait (2013) نشان داده شده است که مصرف‌کنندگان تمایل به اقدامات اضافی برای حفاظت از هویت خود هستند، اما لزوما نمی‌خواهند هزینه اضافی برای این خدمات پرداخت کنند. هدف از این مقاله انتخاب کلمه عبور با توجه به نقاط قوت و اقدامات مختلف برای امن نگه داشتن رمزهای عبور است، ممکن است یک ایده بهتر در میان کاربران "امن‌تر" و "کمتر امن" و تعریف روش احراز هویت متمایزی قرار گیرد. چنین روش احراز هویت متمایزی همه‌ی اطلاعات شناخته شده (استنباط شده از احراز هویت) و یا ارتباط با کاربران بلافاصله پس از سطح اول احراز هویت را شامل می‌شود (به شکل 1 توجه کنید).

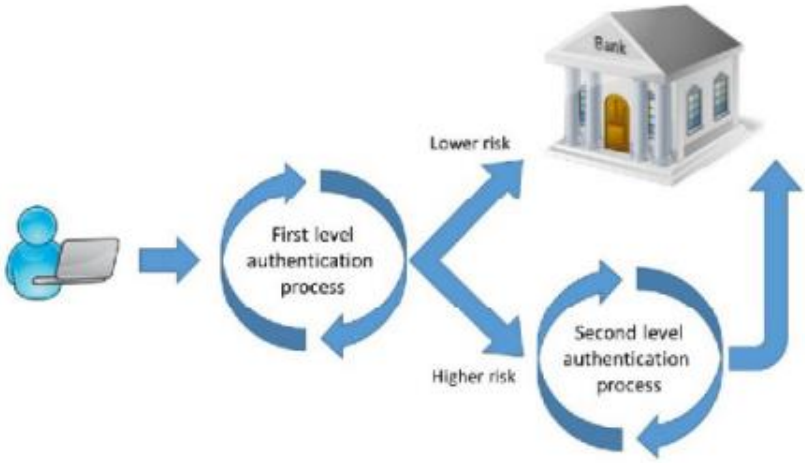

Figure 1: Proposed authentication process

بیش از 9 نفر از هر 10 نفر شرکت کننده در نظرسنجی Ciampa و همکارانش (2013) تمایل خود را برای کار با احراز هویت نام کاربری/ رمز عبور معمول نشان دادند اگر به معنای امنیت قوی‌تر باشد. مصرف‌کنندگان درجه بالایی از پذیرش برای احراز هویت مبتنی بر خطر را با 73 درصد تمایل مثبت نسبت به ارزیابی سازمانی هویت کاربر براساس چیزهایی مانند ورود ، آدرس IP، و رفتار تراکنش نشان دادند.

7. مشکل تحقیقات و هدف

ارائه‌ی یک روش احراز هویت متفاوت وابسته است به (1) توانایی بین شیوه‌های مختلف امنیت کاربران و (2) توانایی منحصر به فرد شناسایی کاربر یا استفاده از گروه، برای اعمال اقدامات اضافی. بالا بردن شرایط ورود اضافی، پس از شناسایی اولیه پیچیده نیست چرا که عمل شناسایی ویژگی‌های خاصی برای کاربران فراهم می‌کند که می‌تواند برای استنباط خطر مورد استفاده قرار گیرد. مورد جالب‌تر، استفاده از اطلاعات شناخته شده در و یا حتی قبل از احراز هویت است. اگر شناسایی ویژگی‌های گروه‌های کاربری امکان‌پذیر باشد ارتباط به شیوه‌های امنیتی صورت خواهد گرفت. این مسئله منجر به سوال می‌شود که اولویت مرورگر به‌طور بالقوه نشان‌دهنده وضع اساسی نسبت به امنیت آنلاین است یا نه.

هدف از این مطالعه این بود:

• ایجاد متریک عملکرد از شیوه رمزگذاری کاربران بانکداری آنلاین.

• اگر تفاوتی در عملکرد، براساس جستجو در انتخاب وجود داشته باشد، ارتباط شیوه‌های آنها با جستجو اولویت و تجزیه و تحلیل مرتفع می‌شود.

اگر تفاوتی در رفتار وجود داشته باشد، یک فرصت برای بالا بردن روش‌های مختلف احراز هویت براساس خطر مرتبط با جستجو استفاده شده فراهم می‌کند.

8. روش

8.1. نظرسنجی

داده‌ها با استفاده از توزیع یک نظرسنجی آنلاین جمع‌آوری شده است. ابزار طراحی شده و از طریق دو تکرار آزمایش به کار برده شده است. نظرسنجی شامل پرسش‌های برای تعیین است:

• عملکرد رمز عبور: با سنجش دانش و توانایی پاسخ دهندگان، انگیزه اندازه‌گیری عملکرد بالقوه می‌تواند ساخته شود.

• اطلاعات دموگرافیک: جمع‌آوری اطلاعات جمعیتی که می‌تواند وابسته به عملکرد رمز عبور باشد.

• استفاده از جستجو: تعیین جستجو استفاده شده توسط پاسخ‌دهندگان.

این نظرسنجی از طریق ایمیل به یک پایگاه داده آنلاین از کاربران آفریقای جنوبی از طریق مؤسسه آموزش عالی و نیز از طریق محققان توزیع شده است.

8.2. نمونه‌ای از پاسخ‌دهندگان

از مجموع 914 نظرسنجی 791 پاسخ دریافت شد. بیشتر از 54 پاسخ‌دهندگان از بانکداری اینترنتی استفاده نمی‌کردند که یک نمونه از 737 پاسخ معتبر ایجاد می‌کند. اطلاعات دموگرافیک برای تعیین بایاس نمونه تحلیل شدند و مشخص شد که ترازی قابل قبول بین کاربران آنلاین جمعیت شناخته شده آفریقای جنوبی و جمعیت نمونه وجود دارد.

8.3. ساختار عملکرد

تابع استفاده شده برای عملکرد توسط McCloy، Campbell و Cudeck (1994) مانند ساختار اصلی برای اندازه‌گیری عملکرد بالقوه استفاده می‌شود. McCloy و همکارانش (1994) عملکرد (PC) را مانند تابعی از دانش اعلانی (DK)، مربوط به یک کار، قابلیت کاربر برای انجام وظیفه (PKS) و انگیزه (M) تعریف کردند: PC=f(DK, PKS, M). عملکرد رمز عبور کاربر کامپیوتر به عنوان یک تابع از سه بخش تشکیل شده است:

- دانش: دانش، آموزش، مهارت‌ها و رقابت مربوط به رمز عبور کاربر؛
- توانایی‌ها: استعداد کاربر برای استفاده از دانش مربوط به رمز عبور به هنگام ایجاد و مدیریت کلمات عبور. و
- انگیزه (M): تمایل نهفته در رفتار کلمه عبور کاربر.

دانش پاسخ دهندگان در پرسشنامه بااستفاده از مجموعه‌ای پرسش که دانش آنها را در مورد گذرواژه‌های قوی و ایمن به خوبی حفاظت و به اشتراک‌گذاری رمزهای عبور سنجش می‌کرد آزمایش شده است.

توانایی‌ها پاسخ‌دهندگان با درخواست از آنها برای رتبه‌بندی ترکیب‌های متفاوت رمزهای عبور مورد آزمایش قرار گرفته است. در رتبه‌بندی کلمه عبور، آنها نیاز به نمایش توانایی خود را برای درک عواملی مانند طول رمز عبور، پیچیدگی، مجموعه کاراکترهای مختلف و همچنین کلمات رایج دارند. اگر چه مجموعه‌ای از پنج کلمه عبور مختلف توسط محققان برای سطوح مختلف امنیتی انتخاب شد، قدرت رمزهای عبور مختلف بررسی شد. همچنین از کاربران در مورد به اشتراک گذاری کلمات عبور و آخرین تغییر در رمز عبور بانکداری اینترنتی سوال شد، به‌عنوان مثال، در مورد تغییرات منظم رمز عبور در 12 ماه گذشته از آنها سوال شد.

انگیزه پاسخ‌دهندگان در مورد اولویت‌بندی امنیتی بااستفاده از تجارت امنیت راحت مورد آزمایش قرار گرفت. امنیت به‌عنوان یک اولویت اصلی برای پیش بینی قابل قبول انگیزه برای رفتار ایمن تعیین شد. مجموعه دوم از پرسش کاربران، در مورد عواملی بود که منجر به تغییر در شیوه‌های رمزگذاری می‌شد. به عنوان مثال ساختاری جهت اقدامات و تعاریف متفاوت براساس شاخص انگیزه تعریف شد. در نهایت، تمایل به استفاده از دانش‌های اضافی، مانند دسترسی به اطلاعات حاصل از بررسی و دستورالعمل برای امنیت آنلاین، به عنوان یک عنصر انگیزه استفاده شد.

8.4. تحلیل داده ها

برداشت کاربران در مورد عملکرد رمز عبور براساس شیوه‌های اعمال شده و متریک محاسبه شده برای دانش، توانایی و انگیزه‌ی هر پاسخ‌دهنده تحلیل شده است. تصمیم گرفته شده است که استفاده از مرورگر از انتخاب پاسخ‌دهندگان برای تکمیل بررسی استنباط نشود، بلکه از آنها پرسیده شود که کدام مرورگر را بیشتر استفاده می‌کنند. شکل 2 توزیع فراوانی برای عملکرد را توسط مرورگر ارجح نشان می‌دهد.

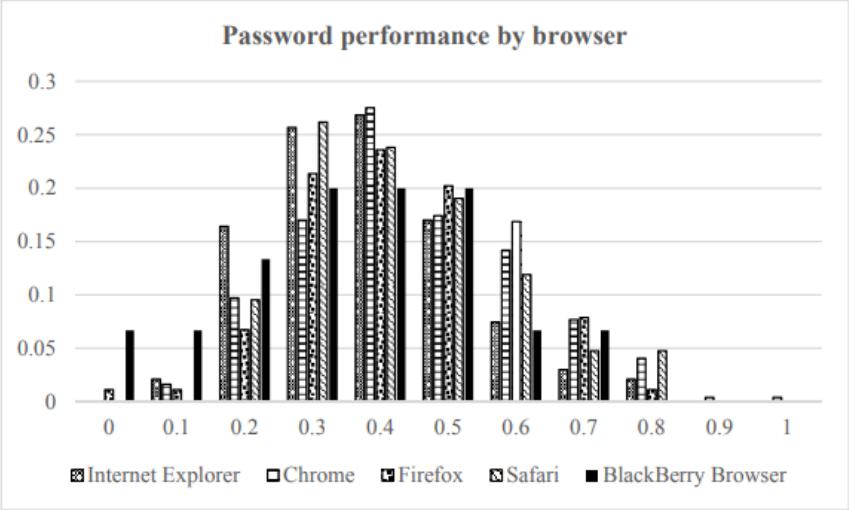

Figure 2: Password performance by survey results

از 737 پاسخ معتبر نمونه‌ی کوچک ، مرورگر BlackBerry (15)، Opera (5)، دیگر / بدون نظر (4) برای پی بردن به نتایج قابل استفاده بدست آمد که در مجموع 708 پاسخ است. میانگین سطح عملکرد رمز عبور برای اینترنت اکسپلورر (0.336) کمتر از کروم (0.394)، فایرفاکس (0.391) و یا سافاری (0.381) است. اما این تفاوت‌های آماری موثر هستند؟

9. عملکرد رمز عبور و انتخاب مرورگر

تجزیه و تحلیل یک طرفه واریانس (ANOVA) برای بررسی تفاوتهای بین دو یا چند گروه ایجاد شده از یک متغیر مستقل واحد مورد استفاده قرار گرفت، به عنوان مثال در عملکرد رمز عبور، در یک متغیر وابسته، مرورگر استفاده

می‌شود. هدف از این تست تصمیم‌گیری این است که آیا تفاوت در میانگین نمرات نمونه برای نتیجه‌گیری این که میانگین نمره گروه نابرابر است به اندازه کافی بزرگ است.

ANOVA تحت مفروضات زیر قابل اعتماد است:

• مقادیر هر یک از گروه‌ها (به‌عنوان کل) از منحنی نرمال پیروی می‌کند،

• با میانگین‌های احتمالا مختلف جمعیت جامعه

• انحراف استاندارد برابر جامعه.

از نظر نرمال بودن، شکل 2 نرمال بودن کافی در داده‌ها برای هر مرورگر و برای انجام آزمون نشان می‌دهد. از نظر واریانس، قاعده کلی این است که بزرگترین نمونه (اینترنت اکسپلورر) بزرگتر از دو برابر کوچکترین نمونه (اپرا) نیست، همانطور که در جدول 2 نشان داده شده است.

فرضیه صفر به عنوان واریانس معنی‌دار بین میانگین نمونه تعریف نشده است، به‌عنوان مثال $H_0: \mu_1 = \mu_2 = \mu_3 = \mu_4$ و فرضیه‌های متناوب به‌عنوان تفاوت معنادار بین میانگین هستند، به عنوان مثال $H_1: \mu_1 \neq \mu_2 \neq \mu_3 \neq \mu_4$. اگر فرضیه صفر درست باشد، "واریانس داخل گروه" با "واریانس بین گروه" مساوی خواهد بود. جدول 2 نتایج حاصل از آزمون آماری واریانس در نمونه برای 95٪ را نشان می‌دهد.

Anova: Single Factor (0.05)

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
Internet Explorer	335	112.6109	0.336152	0.020634
Chrome	247	97.33837	0.394082	0.027622
Firefox	88	34.41523	0.391082	0.021622
Safari	42	15.98869	0.380683	0.023587

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	0.55758	3	0.18586	7.958215	3.1803E-05	**2.61748**
Within Groups	16.53497	708	0.023354			
Total	17.09255	711				

Table 2: One-way ANOVA test for difference between sample means

از آنجا که F (7.96) > Fcrit (2.62)، فرضیه صفر، واریانس معنی‌داری بین میانگین نمونه و در نتیجه استنتاج سطح متفاوتی از عملکرد رمزعبور بر اساس مرورگر مورد استفاده کاربران را رد می‌کند. صرفا با استنتاج مرورگر مورد استفاده کاربر بانکداری آنلاین است انجام احراز هویت مبتنی بر ریسک که توسط Ciampa و همکارانش پیشنهاد شده است عملی نیست (2013).

10. یک مدل متفاوت از تعامل با کاربر

در حالی که برخی از کاربران کامپیوتر ممکن است شیوه‌های رمزگذاری ضعیفی اعمال کنند، مطالعات انجام شده توسط Furnell و همکارانش. (2007)، Riley (2006) و Tam و همکارانش (2010) نشان داد که کاربران دانش تمایز بین شیوه‌های رمزگذاری امن و مطمئن را ندارند. بنابراین یک فرصت برای موسسات مالی جهت ایجاد احراز هویت متفاوت براساس مشخصات پرخطر مشتری وجود دارد. اگر چه آزمایشات انجام شده برای یک عامل شناخته شده در نقطه‌ای از احراز هویت بود، گسترش احراز هویت اولیه (شکل 1) قابل تصور است و همچنین پس از شناسایی

با استفاده از افتراق عوامل که می تواند از اطلاعات دموگرافیک شناخته شده توسط موسسات مالی بدست آید متفاوت خواهد بود.

بهترین اقدام مشترک به‌منظور بهبود عملکرد رمز عبور، آموزش امنیت، آموزش و برنامه‌های آگاهی است (Raily، 2006؛ Furnell و همکارانش 2007: 417). تا به امروز این آموزش برای کاربران به‌صورت داوطلبانه بود. به جای یک الگو متناسب با همه آموزش‌ها، ممکن است به طور مستقیم یک کاربر برای ایجاد یک کلمه عبور قوی جلسه هنگامی که رمز عبور ضعیف تلقی می‌شود آموزش ببیند.

در حال حاضر توصیه نهایی در نظر گرفتن پیغام‌های خطا در سایت‌های بانکی است. حتی پس از احراز هویت، کاربران به‌طور یکنواخت در مورد آخرین کلاهبرداری آنلاین به‌عنوان بخشی از آموزش آگاه می‌شوند. به‌عنوان مثال، ممکن است که کاربر URL را دیده و در مورد کلیک کردن بر روی لینک‌ها به جای تایپ کردن در URL هشدار دریافت کند. بنا به ارتباطات کاربر از طریق استفاده از ریسک‌پذیری، نه تنها پیام مناسب‌تر است، بلکه توجه کاربر به یک پیام طراحی شده جلب می‌شود.

11. محدودیت‌های تحقیق و پیشنهادات

دو محدودیت پیشنهادات و پژوهش حاضر در زیر اشاره شده است:

• احراز هویت متفاوت و ارتباطات پس از آن می‌تواند به عنوان تبعیض تفسیر شود. مفهوم ریسک‌پذیری جدید نیست، اما اگر در طول و بلافاصله بعد از احراز هویت آنلاین به کار گرفته شود می‌تواند توسط کاربران تجربه شود.

• علیرغم وجود تفاوت مشاهده شده در شیوه‌های امنیتی این مسئله اثبات نشده است. تحقیقات بیشتر برای تشخیص میزان و تاثیر تفاوت مورد نیاز است.

• اثر منفی بر حریم خصوصی آنلاین برای کاربران آنلاین

12. نتیجه‌گیری

ادامه نوآوری‌های تکنولوژیکی و رقابت میان بانک‌های موجود و جدید، به محصولات و خدمات بانکی روبه‌رشد منجر شده است. که شامل فعالیت‌های سنتی از جمله دسترسی به اطلاعات مالی، اخذ وام و بازکردن حساب سپرده و همچنین محصولات نسبتا جدید و خدماتی مانند خدمات الکترونیکی پرداخت حساب، پورتال مالی شخصی، تجمع حساب و تغییرات مبادلات کسب و کار به کسب و کار است. وابستگی به تکنولوژی برای ارائه این خدمات نیاز به اطمینان از امنیت لازم برای بانک‌ها و چالش‌های جدید برای تنظیم بانکی دارد.

دنیای آنلاین بنا به پارادوکس ایجاد شده در تلاش برای فایروال‌ها، ممیزی‌های امنیتی و ویروس چکرز است و در عین حال در همان زمان، دسترسی داده شده به یک مرورگر وب اغلب باعث دفاع بیهوده می‌شود. نویسندگان متعدد (Gaur، Patel و Saini، 2013؛ Wahlberg، Paakkola، Wieser، Laakso و 2013Roning) براین باورند که مسائل امنیتی ذاتی در درون مرورگر وجود دارد که می‌تواند مورد سوء استفاده فنی و متفاوت در آسیب‌پذیری به هنگام استفاده از یک مرورگر خاص قرار گیرند. این پژوهش از انتخاب مرورگر به‌عنوان ویژگی کاربران استفاده می‌کند و به دنبال به شناسایی مسائل مرورگر نیست، بلکه تلاش برای درک رفتار کاربر با استفاده از مرورگر انتخاب شده به‌عنوان ویژگی کاربران است. خطرات امنیتی بانکداری اینترنتی همیشه یک نگرانی برای ارائه‌دهندگان خدمات و کاربران بوده است. در مطالعه‌ی عواملی که منجر به تصویب بانکداری آنلاین می‌شود، Yap، Wong، Loh و Bak (2010) مشخص کردند که ویژگی‌های وب‌سایت به مشتریان اعتماد می‌دهد که نشانه وضعیت نرمال قابل توجهی است. استنباط احراز هویت متفاوت می‌تواند به عنوان یک عامل، معقول باشد.

کلمه‌های عبور، شایع‌ترین روش احراز هویت مورد استفاده توسط سیستم کامپیوترها و عوامل انسانی برای در نظر گرفتن اطمینان از امنیت به قوت خود باقی هستند. این تحقیق نشان می‌دهد که استفاده از ریسک‌پذیری برای ایجاد یک سیستم متفاوت احراز هویت کاربران، با استفاده از مرورگر مورد استفاده می‌تواند امنیت آنلاین را بهبود بخشد.

References

Biddle, R., Chiasson, S. and Van Orschot, P.C. (2012), "Graphical Passwords: Learning from the First Twelve Years, ACM Computing Surveys, Vol. 44, No. 4, pp1-19.

Brostoff, S. and Sasse, M.A. (2002), Safe and Sound: a Safety-critical approach to security, Proceedings of the New Security Paradigm Workshop 2001, http://hornbeam.cs.ucl.ac.uk/hcs/people/documents/Angela%20Publications/unsorted/p41- brostoff.pdf, (Accessed 10 April 2014).

Campbell, J., Kleeman, D. and Ma, W. (2007), The good and not so good of enforcing passwords composition rules, Information Systems Security, Vol. 16, No. 1, pp2-8.

Chiasson, S. and Biddle, R. (2007), Issues in User Authentication, CHI Workshop: Security User Studies: methodology and best practices, April.