از تشخیص تقلب تا مدیریت تقلب در شرکت های PSP

مریم نظری دوست، کارشناس شرکت پرداخت نوین آرین، nazaridoustm@gmail.com
سیاوش نظری دوست، کارشناس سازمان تامین اجتماعی، siaolampic@yahoo.com
احمد میردامادی، مدیر عامل شرکت پرداخت نوین آرین، mirdamad0@gmail.com
مازیار جمشیدی، معاونت توسعه بازار و محصول ، jamshidi2621@gmail.com

سومین همایش سالانه بانکداری الکترونیک و نظام های پرداخت

conf.mbri.ac.ir/ebps3

مقدمه

دنیای امروز، دنیای تکنولوژی است و جو حاکم بر زندگی امروز بشر را به سوی مکانیزه کردن و آسانتر کردن وا می دارد. در همین راستا نیز سیستم های پرداخت و بانکداری نیز با تحولاتی شگرف در ساختار های پولی و مالی مواجه شده اند و پول و چک های کاغذی جای خود را به پول ها و چک های الکترونیک و کارت های اعتباری داده اند. با افزایش وابستگی هرچه بیشتر بانک ها و سیستم های پرداخت به کارت های اعتباری و امثال آنها، راه های تقلب در این سیستم ها نیز بیشتر می شود.

تقلب چیست

- تقلب، نوعی سوءاستفاده از منابع، در جهت منافع شخصی، به عمد و کاملاً غیرقانونی است. تقلب در مفهوم عام، عبارت است از تحریف حقایق با اهمیت توسط کسی که میداند مطلبش حقیقت ندارد و یا ارائه حقایق، با کمال بی توجهی نسبت به صحت آنها و به قصد فریب دیگران.
- در تعریف دیگر، واژه تقلب عبارت است از سوءاستفاده از سود یک سازمان بدون اینکه لزوماً به عواقب قانونی آن منجر شود. همچنین، تقلب به فرایندی اشاره دارد که طی آن یک یا چند نفر، عمداً و مخفیانه دیگران را از هر چیز باارزشی، به خاطر منافع شخصی خود محروم کنند.

چالش

سیستمهای مالی مبتنی بر فناوری اطلاعات به دلیل پتانسیل بالایی که در جهت امکان سرقت پولی در حجم بالا دارند اغلب، اهداف راحتی برای حمله کنندگان هستند. متخلفان از نقص احراز هویتهای متعدد و یا نقاط ضعف موجود در مدلهای امنیتی اجراشده در سرویسها استفاده کرده و اهداف خود را پیاده می‌نمایند. احراز هویت ضعیفی که توسط سازوکارهای امضا، پین‌کد، رمز عبور و کد امنیتی کارت اتفاق میافتد، باعث آسان تر شدن تراکنشهای غیرقانونی مالی از طرف حمله کنندگان و از طریق اجرای حملات سیستمی خلاقانه میشود؛ بنابراین می‌بایست از طریق راهکارها، متودولوژی ها و الگوریتم هایی در حوزه آمار، داده‌کاوی و ... تقلب را شناسایی کرد و یا با شناخت الگوها از انجام آنها جلوگیری نمود.

نمونه هایی از تقلب

- کارت ها اعتباری (به خصوص در خریدها و پرداخت های آنلاین)

۱. پول شویی

۲. ایجاد معاملات جعلی به خصوص در خرده فروشی های آنلاین که عموماً توسط پذیرندگان متخلف انجام می شود.

۳. تکرار انجام متوالی عملیات پرداخت یک حواله توسط پذیرنده متخلف در دستگاه‌های POS

نمونه هایی از تقلب های موجود (ادامه)

- تقلب‌های مربوط به پرداخت سیار: این نوع تقلب‌ها به علت ضعف در تکنولوژی سیستم‌های سیار رخ می‌دهد.

۱. تقلب در رومینگ: در برخی از انواع پرداخت های سیار امکان حمله مرد میانی وجود دارد. به عنوان نمونه در پرداخت های مبتنی بر USSD چون BTSاحراز هویت نمی‌شود، خطر وجود BTSهای قلابی وجود دارد و دریافت اطلاعات حساس کاربر وجود دارد.

۲. تقلب مشترک سرویس سیار: به عنوان نمونه مشترک پرداخت های خود را با اطلاعات سیم کارت جعلی یا کاذب یا شبیه سازی شده انجام می دهد به طور کلی مشترک در این حالت به هیچ عنوان قصد پرداخت ندارد. عموماً این مسئله در مورد پرداخت های از نوع اعتباری یا پرداخت های مبتنی بر صورت حساب رخ می‌دهد.

۳. تقلب Tumbing(تاخیر): در این تقلب، متخلف با ایجاد تاخیر، شماره سریال های جعلی را به جریان می اندازد این کار عموماً بر روی گوشی های همسان رخ می‌دهد؛ بنابراین خرابکار می‌تواند یک پرداخت را چندین بار و در تماس های پی در پی انجام دهد.

۴. کلاهبرداری های مالی: ارسال پیام هایی که خبر از برنده شدن‌های جعلی برای کاربر در قرعه کشی یا ... دارند و در نهایت اطلاعات حساس کاربر را مطالبه می کنند.

نمونه هایی از تقلب های موجود (ادامه)

- نفوذ به سیستم: این نوع تقلب ها بر اساس نفوذ به سیستم عمل می کنند، عموماً به این صورت تعریف می شوند که خرابکار به نحوی وارد سیستم کاربر می¬شود. در این روش اغلب متخلف از راه¬هایی برای نفوذ استفاده می کند که کاربر به آن اعتماد داشته باشد و در نهایت اطلاعات مهم مانند شماره حساب و رمز عبور و ... را به دست می آورد. برخی از انواع این نوع تقلب به شرح ذیل است:

۱. کلاهبرداری فیشینگ : ارسال پیامک یا ایمیلی که دارای آدرس یا شماره ای است که بسیار شبیه بانک یا سازمان مورد علاقه کاربر است. در این حالت کاربر اعتماد نموده و اطلاعات حساس خود مانند شماره حساب را ... را فاش می کند.

صحیح	تقلبی
شماره پیامک ۹۰۰۹	شماره پیامک ۹۰۰۹
https://epayment.bmi.ir/MoneyTransfer	https://epayment.bmi.ir/MoneyTransfer@123.23.636

۲. نرم افزار های امنیتی سرکش : این نرم افزارها عموماً در کنار نرم افزارهای مورد اعتماد کاربر قرار می گیرند و به همراه آنها بر روی سیستم کاربر نصب می شوند و اطلاعات کاربر را بدست آورده و برای کامپیوتر خرابکار ارسال می کنند.

۳. پشتیبانی فنی جعلی : در این حالت، خرابکار خود را از طرف یکی از شرکت های بزرگ مانند ماکروسافت و... معرفی می کند و اعلام هشداری را برای کاربر نمایش می دهد به این ترتیب کاربر متقاعد می شود و اجازه نصب نرم افزار یا کنترل کننده را صادر می کند.

نمونه هایی از تقلب های موجود (ادامه)

- سخت افزاری:

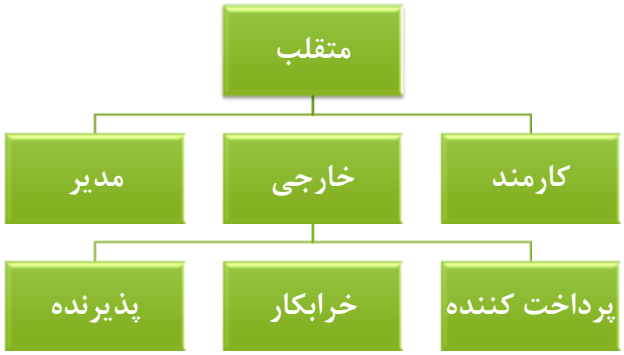
۱. تقلب در خودپرداز: تقلب از طریق خودپردازها از سه طریق سرقت کارت، کپی از اطلاعات کارت ها و یا از طریق نفوذ به ساختار نرم افزاری یا سخت افزاری خودپردازها ممکن می شود.

۲. تقلب در دستگاه های POS و PINPAD

۳. شبیه سازی کارت: در این تقلب، هدف متقلب کپی برداری از اطلاعات کارت‌های بانکی افراد است. به این ترتیب که خرابکار بعد از دریافت اطلاعات کارت فرد با استفاده از خواندن اطلاعات نوار مغناطیسی که در پشت کارت بانکی قرار دارد، اقدام به تهیه کپی از کارت بانکی نموده و از آن در تراکنش‌های بانکی استفاده می‌نمایند.

۴. تغییر در برخی از اطلاعات سخت افزاری و داخلی کارت که عموماً توسط کارمندان ارائه دهنده کارت رخ می دهد و برای تخصیص برخی مجوز های غیر رسمی به کاربران خلافکار بکار می‌رود.

انواع متقلب



تکنیک های شناسایی تقلب

بانک ها و PSPها روش های مختلفی را برای تشخیص تقلب و غربال کردن تراکنش های مشتریان به کار می برند. از جمله ی این روش ها، مشاهده تراکنش ها از طریق سیستم های تصدیق نشانی (AVS)، روش تصدیق کارت (CVM)، شماره شناسایی شخصی (PIN) و روش های زیست سنجی می باشد. AVS شامل شناسایی نشانی از طریق کدهای زیپ شده مشتریان است در حالی که CVM و PIN شامل بررسی عددی است که مشتری به عنوان رمز عبور برای خود در نظر گرفته است. زیست سنجی نیز شامل شناسایی و تصدیق امضا یا اثر انگشت مشتری می شود.

انواع رویکرد های تشخیص تقلب

۱.۲.تشخیص الگوهای سوءاستفاده:

تشخیص سوءاستفاده تلاش می‌کند که حملات مشاهده شده قبلی را در قالب یک الگو و مدل در بیاورد و عموماً از روش-های داده‌کاوی و مجموعه تراکنش های موجود قبلی استفاده می‌کند.

۲.۲. تشخیص ناهنجاری (موارد خلاف قاعده):

در این روش عموماً تلاش می‌شود تا بر اساس برخی از ویژگی‌های خاص تاریخچه عملکردی برای هر کاربر ایجاد و ذخیره شود. در مرحله‌ی بعد، پس از مشاهده‌ی هرگونه انحرافی که به قدر کافی از میانگین ویژگی‌های کاربر فاصله داشته باشد احتمال بروز حمله محاسبه می شود و سیستم امکان بروز یک حمله را به کاربر اطلاع خواهد داد.

❖ **مشکل روش تشخیص عملکرد این است که تنها مبتنی بر تاریخچه‌ی عملکرد یک فرد است و نیاز به گذر زمان و جمع اوری تراکنش های فراوان یک فرد دارد تا بتواند عملکردی مناسب داشته باشد و عموماً دقت این روش نسبت به روش قبل کمتر است.**

تکنیک های شناسایی تقلب

- سیستمهای خبره
- شناسایی موارد پرت
- شبکه های عصبی
- استدلال بر پایه مدل رویکرد مبتنی بر قواعد
- تجزیه و تحلیل حالت گذار
- الگوریتم ژنتیک
- تشخیص ناهنجاری
- روش های فازی
- رگرسیون
- استدلال مبتنی بر مورد (CBR)
- برنامه سازی منطقی استقرایی(ILP)
- رگرسیون
- قوانین وابستگی
- سایر روش های داده کاوی

برخی از تکنیک های ارائه شده در جهان در
روش های تقلب در کارت اعتباری، نفوذ به سیستم و سیستم های سیار

	کارت اعتباری	نفوذ به سیستم	سیار
Outlier Detection	✓		
Neural Network	✓	✓	✓
Anomaly Detection		✓	
Expert System		✓	
Model Based Reasoning		✓	
State Transaction Analysis		✓	
Case Based Reasoning		✓	
Association Rules			✓
Fuzzy Systems	✓		
Virtualization Method			✓
Other Data Mining tech	✓		✓

عملکرد شرکتهای خارجی در حوزه امنیت

لایه امنیت ابزارهای پرداخت و پذیرش (نظیر کارت و دستگاه کارتخوان) ← استاندارد PCI DSS

استاندارد PCI DSS

۱. توسعه و مدیریت یک شبکه مطمئن شامل:

نصب و مدیریت یک برنامه Firewall
عدم استفاده از پارامترهای اولیه نصب‌شده توسط تولیدکننده به عنوان پسورد سیستم

۲. محافظت از اطلاعات دارندگان کارت شامل:

محافظت از اطلاعات ذخیره و آرشیو شده در سیستم
کدگذاری داده‌های مرتبط با اطلاعات انتقال داده شده در شبکه‌های عمومی

۳. استفاده از یک نرم‌افزار به منظور مدیریت ریسک شامل:

استفاده و به‌روزرسانی مداوم نرم‌افزارهای ویروس‌یاب
توسعه و مدیریت سیستم‌ها و برنامه‌های محافظت‌شده

استاندارد PCI DSS(ادامه)

۴. پیاده‌سازی راهکارهای کنترلی شدید در میزان دسترسی به اطلاعات شامل:

محدود کردن دسترسی به اطلاعات دارندگان کارت در حد لزوم

تخصیص یک کد شناسایی مشخص به یک یک افرادی که به اطلاعات دسترسی دارند

ایجاد محدودیت در دسترسی فیزیکی به اطلاعات ذخیره‌شده

۵. کنترل و تست شبکه‌های مورد استفاده شامل:

ثبت و کنترل تمامی ورودها به شبکه‌های حفظ و پردازش اطلاعات دارندگان کارت

اجرای منظم تست سیستم‌ها و رویه‌های امنیت

۶. مدیریت یک سیاست امنیتی در قبال اطلاعات کارتی:

اتخاذ و اجرای سیاستی که حفاظت امنیت اطلاعات توسط تمامی پرسنل را تضمین کند.

عملکرد شرکتهای داخلی در حوزه امنیت

واقعیت آن است که به دلیل رشد بسیار سریع شبکه کارتخوان‌های فروشگاهی کشور و سایر روش‌های پرداخت الکترونیک نظیر پرداخت اینترنتی، لازم است که اکنون با طراحی مجدد این لایه امنیتی تمامی شرکت‌های PSP فعال و نیز تمامی بانک‌های حاضر در کشور ملزم به رعایت استاندارد PCI DSSشده و اقدام به اخذ و ارائه گواهینامه‌های مربوطه در خصوص تمامی ابزارها و تجهیزات خود کنند و به کارگیری هر ابزاری در سطح جامعه منوط به طی فرآیند فوق باشد.

معرفی چند ابزارهای مدیریت تقلب در دنیا

- ✓ سرویس تشخیص تقلب آنلاین ePayAlertتوسط AsiaPay، این سرویس پیشرفته و قابل تنظیم، تراکنش‌های آنلاین را با استفاده گسترده از الگوریتم‌های پویا کنترل و پردازش کرده و همچنین از امکانات گزارش‌دهی و هشدار آنی برخوردار است.
- ✓ برنامه پیشگیری از تقلب در پرداخت‌های الکترونیک آنلاین ReputationManager 360شرکت iovation، این سیستم تا کنون کارکرد ۸۰۰ میلیون قطعه دستگاه پرداخت متعلق به طیف وسیعی از صنایع و مشتری‌ها را زیر نظر دارد و از زمان پیدایش خود بیش از ۶.۵ میلیارد تراکنش آنلاین محافظت کرده است.
- ✓ سیستم مدیریت تقلب فالکون شرکت FICO، این سیستم که ابزار بسیار قدرتمندی جهت جلوگیری از فعالیت متقلبان در سوءاستفاده از کار تهای بدهی و اعتباری میباشد، از الگوریتمهای شبکه عصبی استفاده می کند. این سیستم، احتمال تقلب روی یک حساب را با مقایسه تراکنش جاری و فعالیتهای گذشته دارنده کارت پیش بینی میکند.

معرفی چند ابزارهای مدیریت تقلب در دنیا (ادامه)

- سیستم NIDESشرکت SRIشامل تکنولوژی های داده کاوی به منظور تشخیص ناهنجاری می باشد از جمله ی این تکنیک ها استفاده از قوانین وابستگی است که برای تشخیص سوء استفاده بکار رفته است.
- سیستم (State Transition Analysis Tool) STATشرکت یک سیستم خبره قاعده مدار بسیار معروف است که به منظور جستجوی نفوذهای شناخته شده در یک دنباله ممیزی از سیستم های رایانه ای چندکاربره طراحی شده است.
- PDATیکی از ابزارهای تولید شده با رویکرد مبتنی بر قواعد است که توسط شرکت زیمنس ZFEتهیه شده و ابزاری کاملاً انعطاف پذیر با کاربردی وسیع، به منظور تشخیص تقلب در تلفن های همراه می باشد.

معرفی چند ابزارهای مدیریت تقلب در دنیا (ادامه)

- الگوریتم عصبی MLP، این الگوریتم فقط و فقط روی اطلاعات یک تراکنش و تاریخچه قبل تر از همان تراکنش عمل می‌کند و هیچ نیازی به استفاده از تاریخچه اطلاعات ذخیره شده قبلی دارنده کارت روی بانک اطلاعاتی ندارد.
- سیستم شناسایی تقلب نگین محصول شرکت توسن، این سیستم قابلیت بررسی تمام ورودی ها بر اساس داده های قبلی و تشخیص رفتار غیر متعارف و مشکوک را دارد و با توجه به پیچیدگی رفتار و عملکرد افراد متقلب، نیاز به روش های هوشمند و آموزش پذیر در این سیستم بسیار حساس می باشد و به همین منظور از الگوریتم های متعدد داده کاوی در این سیستم استفاده شده است.
- ماژول امنیتی Anti Fraudشرکت داده ورزی فرادیس البرز، یک قطعه امنیتی است که از نصب ماژول های الکترونیکی خارجی بر روی دریچه ورودی کارتخوان که به منظور کپی کردن و ربودن اطلاعات کارت کاربران استفاده می شوند، جلوگیری می نماید. در واقع با نصب این ماژول امکان نصب قطعات و دستگاه های سرقت اطلاعات به خودپرداز سلب می شود.
- سیستم تشخیص تقلب شرکت ایران پارس پی

سیستم شناسایی تقلب

ایجاد مجموعه ویژگی ها

انتخاب ویژگی ها

تعداد بارهایی که کاربر در هنگام ورود رمز و شناسه به سیستم اشتباه می‌کند (بدون اشتباه، کم اشتباه، چند اشتباه، پر اشتباه و بسیار پر اشتباه)
تعداد پرداخت های اینترنتی (کم، متوسط، زیاد)
مبلغ پرداخت (خرد، متوسط، کلان، خیلی کلان)
زمان یا ساعاتی از شبانه روز که کاربر از سامانه ی مورد نظر استفاده می کند (عادی، کمی غیر عادی، غیر عادی)
نوع کاربر از لحاظ قدمت (تازه وارد، تیمه مسلط، مسلط)
نوع مرورگر از احاظ متدوال بودن و امنیت (نا متداول، نیمه متداول، متداول)
تعداد IPهایی که برای کاربر در هنگام ورود به سیستم ثبت شده است (کم، متوسط، زیاد)
مکان کاربر (برای تراکنش های سیار) از طریق GPS
چقدر تراکنش کاربر با تراکنش های پیشینش مطابقت دارد
مقصد پرداخت
بازه زمانی ای که کاربر برای انجام تراکنش صرف می کند.
نوع رفتار کاربر: امتیاز نهایی از برآیند ویژگی های فوق محاسبه شده و بر طبق آن نوع کاربر حدس زده می شود.

انتخاب سیستم یادگیری مناسب

آموزش الگوریتم یادگیری و ایجاد مدل
ارزیابی مدل

از تشخیص تقلب تا مدیریت آن

دریافت تراکنش جدید

ارسال به مدل

مدل کشف تقلب

رفتار مشکوک

رفتار خیلی مشکوک

رفتار خطرناک

رفتار عجیب

افزایش یک لایه امنیتی مانند (OTP)

جلوگیری از انجام تراکنش تا ۱۰ دقیقه و
افزایش یک لایه امنیتی جدید (OTP)

جلوگیری از انجام تراکنش و غیر فعال کردن کارت

انجام تراکنش

با تشکر

سومین همایش سالانه بانکداری الکترونیک و نظام های پرداخت

۱۶ و ۱۷ دی ماه ۱۳۹۲ – مرکز همایش های برج میلاد

conf.mbri.ac.ir/ebps3