LIBRO BLANCO I OCTUBRE DE 2014

Autenticación 3D-Secure

Los modelos empleados en las transacciones de comercio electrónico para la autenticación basada en riesgos y comportamientos pueden reducir las pérdidas y proporcionar un proceso de compra en línea sin imprevistos para disfrutar de transacciones con bajo riesgo.

Paul Dulany
Hongrui Gong
Kannan Shah
CA Technologies, Advanced Analytics and Data Science

Índice

Resumen ejecutivo 3

Sección 1 4
3D-Secure, la base para reducir las pérdidas en el comercio electrónico

Sección 2 6
Autenticación basada en comportamientos

Sección 3 9
Ventajas de los modelos avanzados

Sección 4 10
Conclusión

Sección 5 10
Acerca de los autores

Resumen ejecutivo

Reto

Las entidades emisoras de tarjetas necesitan equilibrar y compaginar la seguridad en las transacciones de pago del comercio electrónico con una experiencia agradable y ágil para los clientes a la hora de pagar. El quid de la cuestión estriba en cómo ofrecer una experiencia agradable y ágil al pasar por caja para los clientes legítimos, que no les empuje a desistir de la transacción ni optar por otra forma de pago distinta, pero cuidando al mismo tiempo de detener los intentos ilegítimos de realizar transacciones. El empleo de la tecnología de autenticación basada en comportamientos con el fin de determinar en cuáles transacciones es preciso exigir medidas adicionales de autenticación para el cliente es un elemento esencial para reducir los inconvenientes, al tiempo que se garantiza con más seguridad que la transacción es legítima. Para proporcionar este servicio de autenticación basada en comportamientos y riesgos, las reglas son un componente importante. Cuando se añaden modelos y se utilizan como guía para la aplicación de reglas basadas en riesgos, el impacto sobre los intentos de autenticación ilegítimos puede incrementarse notablemente, mientras que las repercusiones sobre los clientes legítimos se reduce. De este modo, el titular de la tarjeta disfruta de una mejor experiencia al tiempo que la entidad emisora reduce sus pérdidas.

Oportunidad

El canal 3D-Secure presenta muchas oportunidades para las entidades emisoras. Dado el notorio incremento en las prácticas fraudulentas dentro del comercio electrónico, sumado a los cambios en las responsabilidades y obligaciones, la tecnología de autenticación 3D-Secure constituye una primera línea de defensa para dichas entidades. Sin embargo, es importante emplear esa primera línea de defensa sabiamente y sacarle el máximo partido. CA Risk Analytics ofrece la oportunidad de examinar las transacciones de comercio electrónico durante la autenticación por medio de información exclusiva, no disponible para los sistemas de detección de fraudes de autorización. Por tanto, permite prevenir las transacciones ilegítimas. Es preciso realizar una evaluación de los riesgos de la autenticación con el fin de proporcionar una experiencia de compra en línea sin interrupciones para la mayoría de los titulares legítimos de tarjetas. Con la ayuda de CA Risk Analytics, las entidades emisoras pueden reducir sus pérdidas y limitar las molestias para los clientes.

Ventajas

CA Risk Analytics puede ayudar a las entidades emisoras a evaluar el nivel de riesgo de las actividades en línea en los sitios web de comerciantes con el protocolo 3D-Secure. Analiza de forma transparente y en tiempo real el riesgo de que el individuo responsable de una transacción de comercio electrónico no sea realmente el titular legítimo de la tarjeta. Puede detectar un número importante de los intentos de realizar transacciones legítimas y permitir que los usuarios continúen sus compras sin que ello les afecte. Al mismo tiempo, sirve para identificar de igual modo los intentos de realizar transacciones ilegítimas que es necesario detener. Identificación de dispositivos, geolocalización, características de conexión y patrones históricos: todos son elementos que es posible contemplar para evaluar el nivel de riesgo de cada intento de transacción.

Un aspecto fundamental de CA Risk Analytics es la disponibilidad de modelos regionales avanzados, con los que se evalúa el nivel de riesgo de un intento de transacción concreto mediante funciones de análisis sofisticadas, incluido un modelo de redes neuronales conductuales, y se obtiene una puntuación que expresa el nivel de riesgo de ese intento. A continuación, las reglas que aplica CA Risk Analytics pueden combinar la puntuación facilitada por el modelo con otros factores de negocio para determinar cuál es la mejor forma de proceder con un intento de transacción concreto. El resultado es un incremento significativo de la eficacia de la solución.

Sección 1

3D-Secure, la base para reducir las pérdidas en el comercio electrónico

El protocolo 3D-Secure abre a las entidades emisoras un mundo repleto de oportunidades que deben aprovechar para sacarle el máximo partido y disfrutar de la protección que ofrece el canal 3D-Secure.

El canal 3D-Secure se centra en la autenticación de los intentos de transacciones de comercio electrónico. Es importante comprender la diferencia entre autenticación y autorización. La autenticación consiste en intentar confirmar que la persona que inicia una transacción (u otra actividad) es el titular de la tarjeta, auténtico y legítimo. La autorización consiste en intentar validar que la persona titular de la tarjeta (confirmada) tiene la autoridad exigible para realizar la transacción (según las políticas, el saldo disponible, el estado de la cuenta y otros tipos de información). Tengamos en cuenta que el fraude se puede producir y detectar tanto en la fase de autorización como en la de autenticación. Ahora bien, existen diferencias clave. Por ejemplo, que la autenticación no combate directamente el fraude en primera instancia. Sin embargo, sea cual sea el tipo de fraude, la autenticación de la persona que pretende realizar una transacción es el primer paso para asegurarnos de que la transacción en sí es válida.

En cuanto a las transacciones con tarjeta presencial, hace ya mucho tiempo que se acepta la presencia física de la propia tarjeta como elemento clave para la autenticación. A medida que los usuarios ilegítimos fueron ganando en sofisticación, las entidades emisoras respondieron mejorando la seguridad de las tarjetas (banda magnética, CVV/CVC/CID y tarjetas inteligentes). Estos datos o los resultados de realizar la autenticación empleando estos datos, se transmiten normalmente con la solicitud de autorización.

En lo que se refiere a las transacciones con tarjeta no presencial (CNP, del inglés “Card Not Present”), resulta imposible la autenticación física por medio de la propia tarjeta. Por regla general, la responsabilidad siempre ha correspondido al comerciante. No obstante, desde la llegada del comercio electrónico, se ha vuelto necesario desarrollar sistemas sólidos de autenticación para el comercio electrónico. Aunque sí son suficientes para autorizar una transacción, los datos de la solicitud de autorización son insuficientes para autenticar una transacción de comercio electrónico. Por lo tanto, así surgió el protocolo de transacción 3D-Secure, con una información distinta de la solicitud de autorización y diseñada para verificar la autenticidad de la persona que intenta realizar una transacción. Esta tarea, que tiene diferencias fundamentales respecto a la autorización, requiere una perspectiva única. Sin embargo, los resultados de esta autenticación se pueden emplear para el proceso de autorización, con el fin de proporcionar un mejor contexto para el sistema de autorización.

Para ser claros: cuando en este documento nos referimos a “fraude”, hablamos de fraude en la autenticación dentro de las transacciones 3D-Secure del comercio electrónico.

Con el protocolo 3D-Secure, existe la oportunidad de examinar los intentos de autenticación de comercio electrónico utilizando información exclusiva no disponible en los sistemas de detección de fraudes en la autorización. Es por ello por lo que permite prevenir una transacción ilegítima antes de que se cree una solicitud de autorización. Al utilizar el sistema CA Risk Analytics, esta información exclusiva incluye un identificador único para cada dispositivo (ID de dispositivo), una URL a la que accede el titular de la tarjeta para realizar la transacción (URL del comerciante), la dirección IP actual del dispositivo e información complementaria de proveedores de datos externos, incluidos la localización del dispositivo, su velocidad de conexión, el tipo y la identificación de anonimizador, así como otra información. Esta información complementa notablemente (pero no sustituye) la información tradicional, como el importe, la divisa, el nombre del comerciante y su identificador, el identificador de la tarjeta y otra información. Gracias a ello, los modelos de autenticación 3D-Secure pueden proporcionar más ventajas que los modelos de autorización que solamente contemplan la información tradicional, ya que incorporan funciones muy eficaces de detección de los intentos de autenticación ilegítimos, al tiempo que limitan sus impactos a un pequeño número de intentos legítimos.

El canal 3D-Secure facilita información en tiempo real para analizar las transacciones de autenticación. Especialmente, tenemos la oportunidad de actualizar información relativa a la tarjeta, al dispositivo o a otras entidades clave que forman parte de la transacción en tiempo real. Esto permite que cualquier transacción subsiguiente aproveche los beneficios de complementar la información y de disponer de contexto cuando se evalúa el nivel de riesgo que entraña la autenticación. Es un recurso especialmente potente si nos fijamos en las entidades bancarias dentro de un entorno SaaS en la nube.

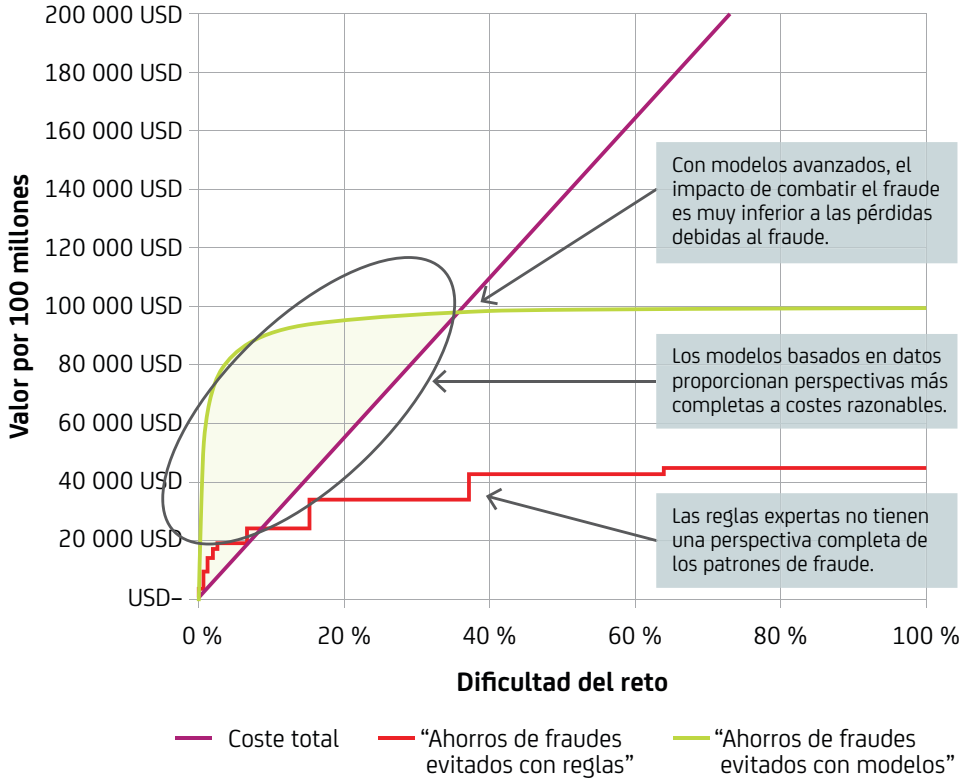
También existe la oportunidad de hacer que la experiencia de compra por comercio electrónico esté libre de molestias. Las implementaciones tempranas de 3D-Secure plantean retos o preguntas a todos los compradores que acuden a sitios web de comerciantes con 3D-Secure. Si el reto planteado es muy exigente, como el uso de contraseñas de un solo uso, puede ser un recurso de eficacia razonable. Si las preguntas que se plantean son excesivamente fáciles, como solicitar información necesaria para realizar la transacción en sí misma (fecha de caducidad o número CVV2 de la tarjeta), será un medio muy deficiente para combatir las pérdidas. Sin embargo, sí existe un efecto secundario: plantear retos desafiantes a los titulares de tarjetas implica molestias o "fricción" durante la transacción, ya que es más complicado concluirla y se ejerce un impacto negativo sobre la experiencia del cliente.

Este efecto adverso en la experiencia del cliente no es puramente cualitativo, sino que también tiene un componente cuantitativo: provoca una notable subida de las tasas de abandono y de "falsos errores". El abandono se traduce en la pérdida de ingresos por tarifas de intercambio, así como en consecuencias de mayor calado, como la pérdida del saldo rotativo de las tarjetas de crédito, además de un posible desgaste o cansancio de los clientes. Esto último constituye un problema relevante tanto para las cuentas de crédito como para las de débito. Estos resultados permiten cuantificar parte del impacto que tiene para las entidades emisoras una experiencia negativa para los clientes y suponen una fuerte motivación para reducir los inconvenientes a la hora de efectuar la transacción. En el caso extremo de plantear el reto o la pregunta a todos los clientes, los costes derivados de los abandonos pueden superar cualquier posible ahorro derivado de las pérdidas evitadas. Por tanto, es esencial evaluar el riesgo de una transacción concreta e intervenir en el proceso solo cuando está plenamente justificado. Lo mejor para ello es aplicar la autenticación basada en comportamientos.

En la página siguiente, la ilustración 1 muestra un ejemplo del coste total de la detección del fraude, incluidas las oportunidades perdidas debido al abandono (línea púrpura), los ahorros logrados con el sistema de reglas convencional (línea roja) y los ahorros de un modelo regional convencional de CA Risk Analytics (línea verde). Fíjese bien en que, a medida que se incrementa la dificultad del reto, también crece el coste de mantener el sistema en marcha. Con un sistema de reglas, en el que no se suele disponer de una perspectiva completa del fraude, el coste de mantener este sistema operativo puede superar rápidamente los ahorros derivados de la aplicación de reglas. Con un modelo avanzado basado en datos, es posible obtener una perspectiva completa del fraude a un coste razonable. La región sombreada en tono verde muestra la ventaja de emplear un modelo respecto a aplicar reglas.

Ilustración 1.

Coste total de la detección de fraudes.



Sección 2

Autenticación basada en comportamientos

La autenticación basada en comportamientos implica analizar la transacción en curso teniendo en cuenta los patrones habituales del titular de la tarjeta, el comerciante y la actividad con el dispositivo de quien efectúa el pago. El objetivo es comprobar si esta información, por sí sola, aporta suficiente confianza de que el pagador es el auténtico titular de la tarjeta. Si es así, no hay necesidad de molestarle en mitad de la transacción y esta puede desarrollarse sin problemas, lo que reduce significativamente las molestias y la probabilidad de abandono. Con ello mejora la experiencia de la que disfruta el titular de la tarjeta[1]. Como alternativa, si casi con total seguridad no se trata del auténtico titular de la tarjeta, se puede denegar directamente la transacción. Así se evitará que se produzca una solicitud de autorización o liquidación y se eliminará la posibilidad de cometer fraude, incluso si su autor dispone de los datos para autenticarse. Por último, para aquellas transacciones en las que no existe una fiabilidad alta sobre su legitimidad o ilegitimidad, sería aconsejable emprender una interacción de autenticación sólida con el titular de la tarjeta. La idea clave en la autenticación basada en comportamientos es utilizar los patrones de conducta para reducir la incertidumbre derivada de si la persona que intenta proceder a la autenticación es o no es el titular legítimo de la tarjeta. Por lo tanto, de forma simultánea, (a) se reduciría el número de transacciones legítimas a las que se añadiría la molestia de autenticarse por segunda vez, (b) se garantizaría que más casos de fraude pasarían por la autenticación secundaria y (c) se denegarían directamente más casos de fraude.

Los modelos sirven como mecanismos autenticadores basados en comportamientos

Los modelos regionales de CA Risk Analytics se crean con datos de entidades emisoras regionales que permiten el empleo de sus datos en CA eCommerce Consortium y que aportan "datos verdaderos"[2]. Dichos datos incluyen transacciones 3D-Secure tanto de tarjetas de débito como de crédito.

Los modelos regionales comprenden una serie de diferentes elementos. En primer lugar, utilizan la información de la transacción actual. Eso incluye la fecha y la hora, el importe, la localización de la persona que intenta autenticarse para realizar una transacción (el equipo o el dispositivo móvil del titular de la tarjeta en el caso del comercio electrónico), el nombre del comerciante, su identificador y URL, información sobre la dirección IP del dispositivos, las características de conexión e información auxiliar procedente de proveedores de datos externos. Esta información es fundamental para que el modelo entienda la transacción actual. Sin embargo, no es suficiente para entender las conductas involucradas.

En segundo lugar, los modelos utilizan información de distintos comportamientos correspondiente a las entidades clave del actual intento de autenticación, como la tarjeta, el dispositivo o el comerciante. La información sobre el comportamiento anterior se refina para extraer los factores importantes para la observación de los patrones de conducta. Aquí se incluye información como: qué comerciantes se han visitado, cantidades e importes, localizaciones y dispositivos utilizados en cada visita, así como qué dispositivos únicos se han utilizado con esta tarjeta. También se buscan patrones similares en otras entidades clave. Estos "puntos clave seleccionados" o refinados, como se denominan los historiales, se actualizan con cada intento registrado de realizar una autenticación para una transacción.

En tercer lugar, los modelos utilizan variables complejas, incluidos minimodelos que aíslan los patrones de comportamiento de los puntos clave involucrados en la transacción. Además, determinan si la transacción actual se atiene a esos patrones y cómo. Estas variables pueden ser algo tan sencillo como identificar si se utiliza un dispositivo nuevo con una determinada tarjeta o medir la velocidad de gasto correspondiente a una tarjeta o dispositivo. Sin embargo, también pueden ser complejas, como comparar la tendencia que presenta un determinado titular de tarjeta de repetir las compras y cuántas veces ha visitado el sitio web de un comerciante frente a los datos equivalentes de otras personas.

En cuarto lugar, los modelos se sirven de tablas creadas con datos históricos. Estas tablas proporcionan información sobre tendencias pasadas de transacciones legítimas y fraudulentas en los datos históricos, incluidas estadísticas de tendencias y Naïve Bayes.

Finalmente, todos estos elementos distintos se facilitan a un modelo numérico no lineal que compara y sopesa sus diferentes predicciones considerando las anomalías de la conducta y el riesgo de que se produzcan intentos ilegítimos. Estos modelos capturan los comportamientos no lineales: las relaciones importantes entre variables y la probabilidad de que se produzca fraude, elementos que no constituyen una simple relación lineal. Comparan indicadores de riesgo con factores atenuantes (se trata aquí de un comerciante con un alto volumen de fraude por importes elevados, pero esta persona ha realizado anteriormente este mismo tipo de transacción desde este dispositivo), fijándose en muchas relaciones distintas.

La manera en que se comparan y compensan los diferentes factores se determina aplicando un algoritmo de entrenamiento sobre un gran conjunto de datos de transacciones históricas y los "datos verdaderos". Por tanto, estos tipos de modelos se basan de forma inherente en los datos. Esto permite que los modelos "detecten" las relaciones no triviales que no son tan fáciles de capturar con las reglas. A continuación, facilita el cálculo más aproximado de la probabilidad de que se trate de una transacción ilegítima.

La productividad de estos modelos es una cifra que proporciona una estimación de la probabilidad de que ese intento concreto de autenticación sea *ilegítimo.* Así se admite una clasificación por orden de las transacciones de autenticación, lo que permite adoptar distintas medidas y asignar prioridades dentro de esas actuaciones. En particular, se hace posible la "autenticación silenciosa" de las transacciones sin causar molestias al titular de la tarjeta, basándose en los patrones de comportamientos anteriores registrados en los datos, que señalan una baja probabilidad de prácticas ilegítimas.

Uso de modelos numéricos no lineales con redes neuronales feed-forward

Entre las numerosas variantes distintas del uso de modelos numéricos que hay disponibles, las redes neuronales feed-forward (FFNN) proporcionan una combinación ideal de rendimiento, flexibilidad y viabilidad.

Las redes neuronales feed-forward son extremadamente flexibles, ya que no requieren ninguna asunción estructural o distributiva que afecte al espacio de característica de entrada. Se caracterizan por ofrecer un rendimiento a la última incluso con los datos con características de no linealidad más acusadas, ya que son aproximadores de función universal. Además, independientemente del tamaño o la complejidad de los datos, se entrenan en tiempo lineal, lo cual las convierte en una solución muy práctica, incluso para conjuntos de datos extraordinariamente grandes.

Estructura de las redes neuronales

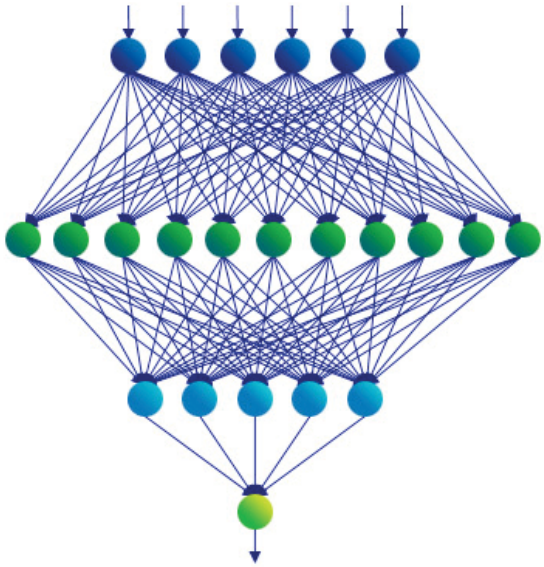
En esencia, una red FFNN es un gráfico de flujo de señales no lineales acíclico y dirigido, cuyo valor de entrada es una representación numérica de la transacción registrada por medio de las técnicas mencionadas anteriormente, y cuyo valor de salida en este contexto se interpreta como una medición ordinal de la probabilidad de que el intento de autenticación sea fraudulento (la puntuación).

En un enfoque más descriptivo, podemos describir las redes FFNN como compuestas por una secuencia de “capas”, cada una de ellas formada por un conjunto de “neuronas” (véase la ilustración 2). El intento de autenticación de la entrada se presenta a la primera capa (de entrada), donde comienza su propagación por toda la red. Esta propagación continúa a través de las capas internas (“capas ocultas”), hasta por último llegar a la capa de salida. Cada capa ejecuta una transformación no lineal sobre su entrada y transfiere el resultado a la capa subsiguiente. Cada capa puede contener un número arbitrario de neuronas, pero en el contexto actual, la capa final (de salida) solamente cuenta con una única neurona (que calcula la puntuación).

El potencial expresivo de las redes FFNN se asienta sobre estas transformaciones no lineales secuenciales, que colectivamente confieren a la red FFNN la capacidad de modelar cualquier función del valor de entrada que reciben.

Ilustración 2.

Ejemplo de red neuronal feed-forward (FFNN).



Sección 3

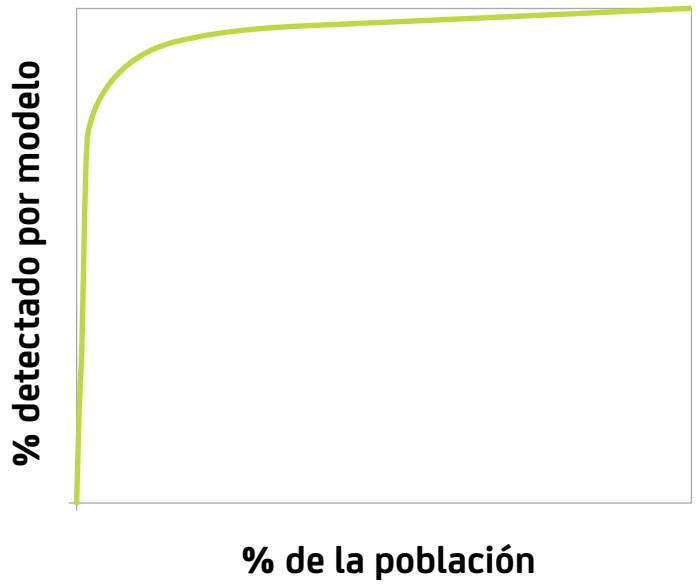
Ventajas de los modelos avanzados

Rendimiento de los modelos

Los modelos de CA Regional Models permiten aplicar la denegación o ampliación de la autenticación sobre la mayoría de las transacciones fraudulentas, al tiempo que solamente impactan sobre un número limitado de transacciones legítimas. El rendimiento general se indica en la ilustración 3. El modelo potencia al máximo la detección de los casos de fraude, reduciendo simultáneamente al mínimo el impacto para los clientes. Tenga en cuenta que el gráfico no muestra la curva completa, sino que se centra en su área operativa.

Ilustración 3.

Detección de fraude del modelo, expresada en función del porcentaje de todas las transacciones marcadas por el modelo. Tenga en cuenta que el gráfico está centrado en el área operativa de la curva y solamente muestra una porción de la población.



Puntuaciones y reglas de los modelos

Las reglas son un gran recurso para atacar indicadores precisos y bien conocidos de fraude. Se implementan rápidamente y son fáciles de entender. Ahora bien: no tienen los datos como motor, así que están limitadas por los conocimientos sobre posibles señales de fraude que tiene quien las escribe. Las reglas no pueden capturar con facilidad comportamientos complejos y no facilitan la tarea de contemplar y combinar varios riesgos de cara a tomar una única decisión. Por último, no tienen la capacidad de clasificar por orden las transacciones para permitir que se ajusten los volúmenes de intentos con resultado de denegación, de autenticación secundaria y considerados como casos de estudio.

Los modelos detectan y registran patrones complejos sirviéndose de variables sofisticadas. Las variables se basan en la transacción actual, así como en los puntos clave seleccionados y procesados (información fundamental de transacciones pasadas sobre elementos identificadores cruciales en las transacciones, que ha sido refinada). Con el uso de variables lineales y también no lineales, además de técnicas de entrenamiento establecidas, los modelos permiten compensar diferentes factores utilizando un enfoque cuyo motor son los datos. Así ofrecen una clasificación por orden de las transacciones, basada en la probabilidad de que sean casos de fraude. Sin embargo, los modelos no emprenden acciones por sí mismos; las reglas son un complemento esencial para ellos.

Uso conjunto de reglas y modelos

A la vista de las distintas fortalezas que caracterizan a modelos y reglas, el mejor enfoque es aplicar los dos elementos juntos. En primer lugar, utilizar un modelo robusto para diferenciar los casos de fraude de aquellos que no lo son y clasificar las transacciones con una puntuación. En segundo lugar, escribir reglas que utilicen esta puntuación de varias maneras: (i) puntuaciones altas indican que la probabilidad de fraude es alta y deberían dar pie a que se emprendan acciones, con un ajuste del umbral de puntuación para lograr los volúmenes y la riqueza de control del fraude que la institución se plantee como objetivos; además, (ii) las puntuaciones más bajas se pueden usar en conjunción con reglas antifraude de tipo flash u otras reglas, para filtrar y excluir aquellas que presenten una elevada probabilidad de no tener carácter fraudulento y permitir que las reglas se apliquen en un conjunto de datos más rico. Por último, habrá reglas de políticas, que son independientes de la probabilidad del fraude y que implementa la institución. Tal vez requieran una autenticación secundaria para los nuevos dispositivos, sea cual sea la probabilidad de fraude.

Sección 4

Conclusión

El empleo de la tecnología de autenticación basada en comportamientos con el fin de determinar qué transacciones deberían recibir el impacto de la autenticación o la denegación resulta esencial para reducir los impactos sobre los clientes (es decir, las molestias) mientras se garantiza con más seguridad que la transacción es legítima. Para proporcionar este servicio de autenticación basada en comportamientos y riesgos, las reglas son un componente importante. Sin embargo, también tienen ciertas limitaciones. Cuando se añaden modelos sofisticados basados en comportamientos y se utilizan como guía para la aplicación de reglas basadas en riesgos, el impacto sobre los intentos de autenticación ilegítimos puede incrementarse notablemente, mientras que el impacto sobre los clientes legítimos se reduce. De este modo, el titular de la tarjeta disfruta de una mejor experiencia, mientras que la entidad emisora reduce sus pérdidas.

Sección 5

Acerca de los autores

Paul Dulany lleva 14 años trabajando en el área de la analítica avanzada y la ciencia de los datos. Entró a formar parte de CA Technologies en 2013 y dirigió el desarrollo de la infraestructura de modelado analítico, así como del primer modelo producido por el equipo CA Data Science. Antes de trabajar para CA Technologies, estuvo ocho años en el SAS Institute, donde formó parte del equipo que desarrolló los primeros modelos para la solución de gestión antifraude SAS Enterprise Fraud Management, además de liderar el desarrollo de los primeros modelos para tarjetas de débito y desarrollar muchas nuevas técnicas. Antes de su etapa en SAS, Paul trabajó para HNC y Fair Isaac durante más de cinco años, primero como científico y posteriormente como gestor del equipo de modelado de Fraud Predictor. Durante este período desarrolló varios modelos para tarjetas de pago Falcon, además de trabajar en otros ámbitos. Paul es titular de varias patentes, derivadas de su época en HNC y SAS, además de ser doctor en física teórica.

Hongrui Gong tiene una amplia experiencia en el ámbito de la analítica avanzada y la ciencia de los datos. Empezó a trabajar para CA Technologies en abril de 2013 y desempeñó un papel clave en los esfuerzos por construir una infraestructura de modelado y desarrollar modelos para productos 3D-Secure. Antes de llegar a CA, pasó más de 15 años trabajando con empresas de primera línea especializadas en tecnologías de análisis (SAS, FICO y HNC), donde participó en el desarrollo de modelos para productos como la detección de fraude relacionado con tarjetas de pago, detección de fraudes de seguros, identificación de evasores fiscales para gobiernos regionales y nacionales, sistemas contra el blanqueo de capitales, previsión de impagos en préstamos, gestión de riesgos de ingresos por márgenes de intermediación

y calificación de nivel de riesgo crediticio para corporaciones públicas y privadas. Hongrui es doctor en dinámica de fluidos computacional y pasó cuatro años en Los Alamos National Laboratory, dedicado a investigar sobre la creación de modelos teóricos y simulaciones informáticas de los flujos de fluidos turbulentos. Es titular de varias patentes, derivadas de sus anteriores experiencias laborales.

Kannan Shah lleva seis años trabajando en el sector de la analítica avanzada y la ciencia de los datos. Entró a formar parte de CA Technologies en 2013 y dirigió el desarrollo de la infraestructura de modelado analítico, así como del primer modelo producido por el equipo CA Data Science. Antes de entrar a formar parte de CA Technologies, fue científico principal del SAS Institute, donde desarrolló técnicas y modelos estadísticos, además de proporcionar asistencia a clientes para la solución de gestión antifraude SAS Enterprise Fraud Management. Ha contribuido al desarrollo de modelos de detección de fraudes para tarjetas de pago, transferencias bancarias y transferencias por CCA; implementados en Estados Unidos, el Reino Unido, México y la región Asia-Pacífico. Kannan es titular de varias patentes, derivadas de su trabajo en SAS. Posee un título de maestro en ingeniería eléctrica de la Drexel University de Filadelfia. Durante sus estudios académicos, se especializó en disciplinas como la detección y la estimación, el procesamiento de señales estocástico, la inteligencia artificial, el reconocimiento de patrones estadísticos, las redes neuronales, la teoría de la información, el análisis espectral de orden superior y el diseño y la complejidad de algoritmos.

ca technologies

Comuníquese con CA Technologies en ca.com/es.

CA Technologies (NASDAQ: CA) crea software que impulsa la transformación de las empresas y les permite aprovechar las oportunidades que brinda la economía de las aplicaciones. El software se encuentra en el corazón de cada negocio, en todos los sectores. Desde la planificación hasta la gestión y la seguridad, pasando por el desarrollo, CA trabaja con empresas de todo el mundo para cambiar la forma en que vivimos, realizamos transacciones y nos comunicamos, ya sea a través de la nube pública, la nube privada, plataformas móviles, entornos de mainframe o entornos distribuidos. Para obtener más información, visite **ca.com/es**.

1 En las regiones donde se ha desarrollado una labor educativa significativa para instruir a los titulares de tarjetas para que busquen los indicadores de 3D-Secure, es posible reforzar la confianza del titular si aparece una ventana desplegable que anuncie que la transacción está protegida con 3D-Secure.

2 El término “datos verdaderos” se refiere a la información de la tarjeta y de la transacción que permite identificar las transacciones que el proceso de autenticación debería detener.

Copyright © 2014 CA. Todos los derechos reservados. Todas las marcas, nombres comerciales, logotipos y marcas de servicio a los que se hace referencia en este documento pertenecen a sus respectivas empresas. El propósito de este documento es meramente informativo. CA no se responsabiliza de la precisión e integridad de la información. En la medida de lo permitido por la ley vigente, CA proporciona esta documentación “tal cual”, sin garantía de ningún tipo, incluidas, a título enunciativo y no taxativo, las garantías implícitas de comerciabilidad, adecuación a un fin específico o no incumplimiento. CA no responderá en ningún caso de las pérdidas o daños, directos o indirectos, que se deriven del uso de esta documentación, incluidas, a título enunciativo y no taxativo, la pérdida de beneficios, la interrupción de la actividad empresarial, la pérdida del fondo de comercio o la fuga de datos, incluso cuando CA hubiera podido ser advertida con antelación y expresamente de la posibilidad de dichos daños. CS200_94860_1014