WHITE PAPER | OKTOBER 2014

3-D Secure-Authentifizierung mit erweiterten Modellen

Modelle, die für die risiko- oder verhaltensbasierte Authentifizierung von eCommerce-Transaktionen verwendet werden, können Verluste verringern und bei Transaktionen mit geringem Risiko eine reibungslose Kaufabwicklung ermöglichen.

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

ca technologies

Inhaltsverzeichnis

Kurzfassung

Ausgangssituation

Aussteller müssen ein Gleichgewicht zwischen der Sicherheit von eCommerce-Bezahltransaktionen und einer problemlosen Kaufabwicklung für die Kunden schaffen. Der Knackpunkt dabei ist, legitimen Kunden eine nahtlose Kaufabwicklung zu ermöglichen, sodass sie ihre Transaktion nicht abbrechen oder eine andere Zahlungsmethode verwenden, während gleichzeitig illegitime Transaktionsversuche unterbunden werden müssen. Der Einsatz einer verhaltensbasierten Authentifizierung, um die Transaktionen zu bestimmen, bei denen die Kunden eine zusätzliche Authentifizierung durchlaufen müssen, ist entscheidend, um Reibungspunkte bei Kunden zu vermeiden und besser zu gewährleisten, dass die Transaktion legitim ist. Regeln sind eine wichtige Komponente für diese risiko- und verhaltensbasierte Authentifizierung. Wenn Modelle hinzugefügt werden und die Anwendung risikobasierter Regeln vorgeben, kann der Einfluss auf illegitime Authentifizierungsversuche beträchtlich erhöht werden. Gleichzeitig werden die Auswirkungen auf legitime Kunden verringert, sodass die Erfahrungen für den Karteninhaber optimiert und die Verluste für den Aussteller verringert werden.

Chancen

3-D Secure bietet Ausstellern viele Chancen. Durch die enorme Zunahme bei eCommerce-Betrug und die Veränderungen bei der Haftung stellt die 3-D Secure-Authentifizierung eine erste Verteidigungslinie für Aussteller dar. Sie sollte jedoch klug und möglichst vorteilhaft genutzt werden. CA Risk Analytics bietet die Chance, eCommerce-Transaktionen während der Authentifizierung zu untersuchen. Dazu werden eindeutige Informationen genutzt, die Systemen zur Erkennung von Autorisierungsbetrug nicht zur Verfügung stehen. Auf diese Weise kann eine illegitime Transaktion verhindert werden. Das Authentifizierungsrisiko muss bewertet werden, um der Mehrheit legitimer Karteninhaber eine störungsfreie Kaufabwicklung zu ermöglichen. Ist CA Risk Analytics installiert, können Aussteller Verluste reduzieren und Reibungspunkte für Kunden beschränken.

Nutzen

Mit CA Risk Analytics können Aussteller das Risiko von Onlineaktivitäten bei 3-D Secure-Händlern bewerten. Damit wird transparent und in Echtzeit das Risiko beurteilt, ob der Versuch einer illegitimen eCommerce-Transaktionsabwicklung – also nicht von legitimen Karteninhabern – unternommen wird. Die Lösung kann einen beträchtlichen Teil legitimer Transaktionsversuche identifizieren und es Kunden ermöglichen, den Einkauf ohne Störungen fortzusetzen, während illegitime Transaktionsversuche erkannt werden, die beendet werden sollten. Geräteidentifikation, geografischer Standort, Verbindungsmerkmale und protokollierte Muster können zur Beurteilung des Risikos jedes Transaktionsversuchs herangezogen werden.

Ein kritischer Aspekt von CA Risk Analytics ist die Verfügbarkeit erweiterter regionaler Modelle, mit denen das Risiko eines bestimmten Transaktionsversuchs über ausgereifte Analysen wie verhaltensbasierter Modelle neuronaler Netze bewertet wird. Eine Bewertung gibt dann an, welches Risiko der Versuch darstellt. Mit Regeln in CA Risk Analytics kann diese Modellbewertung anschließend mit anderen geschäftlichen Faktoren kombiniert werden, um die beste Behandlung eines bestimmten Transaktionsversuchs zu ermitteln. Dadurch wird die Effektivität der Lösung beträchtlich gesteigert.

Abschnitt 1

3-D Secure als Basis für Verlustreduzierung bei eCommerce

Das 3-D Secure-Protokoll bietet Ausstellern viele Chancen, die ergriffen werden müssen, um alle Vorteile und den Schutz von 3-D Secure zu nutzen.

Der Fokus von 3-D Secure liegt auf der Authentifizierung von eCommerce-Transaktionsversuchen. Es ist wichtig, den Unterschied zwischen Authentifizierung und Autorisierung zu kennen. Authentifizierung ist der Versuch zu bestätigen, dass die eine Transaktion (oder sonstige Aktivität) startende Person der legitime und echte Karteninhaber ist. Autorisierung ist der Versuch zu überprüfen, ob der (bestätigte) Karteninhaber zur Transaktion autorisiert ist. Dazu werden Richtlinien, verfügbare Salden, der Kontostatus und andere Informationen genutzt. Betrug kann in den Autorisierungs- und Authentifizierungsschritten erkannt werden, es bestehen aber wichtige Unterschiede. Beispielsweise wird bei der Authentifizierung interner Betrug nicht direkt berücksichtigt. Unabhängig vom Betrugstyp ist die Authentifizierung der Person, die eine Transaktion ausführen möchte, der Ausgangspunkt bei der Sicherstellung, dass die Transaktion selbst zulässig ist.

Bei direkten Kartentransaktionen wurde das physische Vorhandensein der Karte lange als eine Schlüsselkomponente der Authentifizierung akzeptiert. Auf die zunehmende Raffinesse illegitimer Anwender haben die Aussteller mit besserer Sicherheit der Karten (Magnetstreifen, CVV/CVC/CID und Smartcards) reagiert. Diese Daten bzw. die Ergebnisse der Authentifizierung mit diesen Daten werden im Allgemeinen bei der Autorisierungsanforderung weitergeleitet.

Bei Transaktionen ohne physische Karte (Card Not Present, CNP) ist eine physische Authentifizierung über die Karte nicht mehr möglich, und die Haftung liegt im Allgemeinen beim Händler. Durch das Aufkommen von eCommerce wurde es allerdings erforderlich, eine zuverlässige Authentifizierung von eCommerce-Transaktionen zu entwickeln. Die Daten der Autorisierungsanforderung sind zwar für die Autorisierung einer Transaktion ausreichend, sie reichen aber nicht für die Authentifizierung einer eCommerce-Transaktion aus. Dies war die Geburtsstunde der 3-D Secure-Transaktion, bei der andere Informationen als die Autorisierungsanforderung verwendet werden und die für die Authentifizierung der Person konzipiert wurde, die eine Transaktion durchführen möchte. Diese Aufgabe, die sich grundlegend von der Autorisierung unterscheidet, erfordert eine eindeutige Perspektive. Jedoch können die Ergebnisse dieser Authentifizierung bei der Autorisierung verwendet werden, um dem Autorisierungssystem einen besseren Kontext zur Verfügung zu stellen.

Zur Präzisierung: Wenn wir in diesem Dokument von Betrug sprechen, meinen wir Authentifizierungsbetrug bei 3-D Secure-Transaktionen im Bereich eCommerce.

Mit dem 3-D Secure-Protokoll gibt es die Chance, eCommerce-Authentifizierungsversuche mit eindeutigen Informationen zu untersuchen, die in Systemen zur Erkennung von Autorisierungsbetrug nicht vorliegen. Dadurch kann eine illegitime Transaktion verhindert werden, bevor von ihr eine Autorisierungsanforderung erstellt wird. Beim CA Risk Analytics-System zählen zu den eindeutigen Informationen: eine eindeutige ID für jedes Gerät (Geräte-ID), ein URL, auf den der Karteninhaber für die Transaktion zugreift (Händler-URL), die aktuelle IP-Adresse des Geräts und Zusatzinformationen von externen Datenanbietern wie Gerätestandort, Verbindungsgeschwindigkeit, Typ und die Identifikation von Anonymisierern sowie sonstige Informationen. Mit diesen Informationen werden die herkömmlichen Informationen wie Betrag, Währung, Händlername und Händler-ID, Karten-ID und sonstige Informationen beträchtlich erweitert (aber nicht ersetzt). Durch diese Erweiterung können 3-D Secure-Authentifizierungsmodelle einen größeren Nutzen bieten als Autorisierungsmodelle, die nur die herkömmlichen Informationen nutzen. Sie ermöglichen eine zuverlässige Erkennung illegitimer Authentifizierungsversuche, haben aber nur auf einen kleinen Teil der legitimen Versuche Einfluss.

3-D Secure stellt in Echtzeit Informationen für die Analyse von Authentifizierungstransaktionen bereit. Insbesondere haben wir die Möglichkeit, Informationen zu Karte, Gerät oder anderen zentralen Einheiten in der Transaktion in Echtzeit zu aktualisieren. Dadurch können nachfolgende Transaktionen vom Nutzen von mehr Informationen und Kontext profitieren, wenn sie im Hinblick auf Authentifizierungsrisiken beurteilt werden. Dies kann bei Einheiten von Banken in einer Cloud-Umgebung mit Software-as-a-Service (SaaS) besonders leistungsfähig sein.

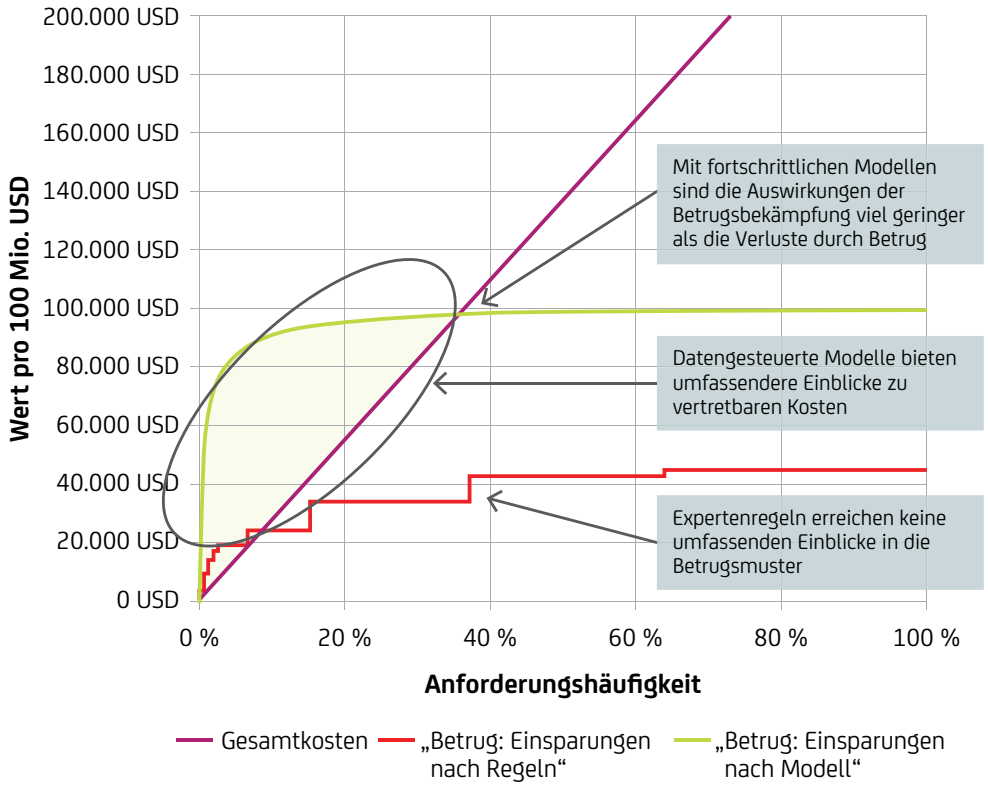
Darüber hinaus besteht die Chance, den eCommerce-Einkauf relativ reibungslos zu gestalten. Frühe 3-D Secure-Implementierungen stellen allen Käufern bei 3-D Secure-Händlern prüfende Fragen. Wenn die Frage schwierig ist, beispielsweise bei Einmal-Passwörtern (One-Time-Passwords, OTP), kann dies einigermaßen effektiv sein. Sind die prüfenden Fragen aber einfach, weil sie sich auf Informationen beziehen, die für die eigentliche Transaktionsabwicklung erforderlich sind (Ablaufdatum oder CVV2), trägt dies wenig zur Bekämpfung von Verlusten bei. Es gibt jedoch noch einen zweiten Effekt: Durch prüfende Fragen an die Karteninhaber entstehen „Reibungspunkte“ in der Transaktion – der Widerstand gegen einen Transaktionsabschluss nimmt zu und beeinflusst die Customer Experience negativ.

Der negative Einfluss von Reibungspunkten auf die Customer Experience ist nicht nur qualitativ, sondern auch quantitativ: Dadurch steigen die Abbrüche und die Raten „falscher Fehler“ deutlich. Abbrüche führen zu entgangenen Abwicklungsgebühren sowie zu größeren Auswirkungen wie Verlusten der revolvierenden Kreditlinie von Kreditkarten oder möglichen Kundenabwanderungen, was bei Schuld- und Guthabenkonten ein großes Problem ist. Durch diese Auswirkungen kann ein Teil des Einflusses einer negativen Customer Experience auf den Aussteller quantifiziert werden und stellt eine starke Motivation zur Verringerung von Reibungspunkten in der Transaktion dar. Im extremen Fall der Prüfung aller Kunden können die Kosten von Abbrüchen mögliche Verlustverringerungen aufwiegen. Daher ist es entscheidend, das Risiko einer bestimmten Transaktion zu beurteilen und nur bei einer guten Rechtfertigung in den Prozess einzugreifen. Optimal ist dafür die verhaltensbasierte Authentifizierung.

Abbildung 1 auf der folgenden Seite veranschaulicht ein Beispiel der Gesamtkosten für die Betrugserkennung, einschließlich entgangener Chancen aufgrund von Abbrüchen (lila), die Einsparungen eines typischen Regelsystems (rot) und die Einsparungen eines typischen regionalen CA Risk Analytics-Modells (grün). Dabei steigen mit der Prüfungsrate die Kosten für den Systembetrieb. Bei einem Regelsystem, in dem meist ein umfassender Überblick über den Betrug fehlt, können die Kosten des Systembetriebs schnell die Einsparungen durch die Regeln übersteigen. Mit einem erweiterten datengesteuerten Modell kann ein umfassender Überblick über den Betrug zu angemessenen Kosten erreicht werden. Der grünschattierte Bereich zeigt die Vorteile eines Modells im Vergleich zu Regeln.

Abbildung 1.

Gesamtkosten der Betrugserkennung



Abschnitt 2

Verhaltensbasierte Authentifizierung

Bei der verhaltensbasierten Authentifizierung wird die aktuelle Transaktion im Kontext normaler Aktivitätsmuster von Karteninhaber, Händler und Gerät des Zahlers betrachtet, um festzustellen, ob allein anhand dieser Informationen mit großer Sicherheit angenommen werden kann, dass der Zahler auch der authentische Karteninhaber ist. In diesem Fall muss der Zahler nicht während der Transaktion gestört werden. Die Transaktion wird ohne Beeinträchtigung abgewickelt. Dadurch werden Reibungspunkte und die Wahrscheinlichkeit eines Abbruchs deutlich reduziert, sodass sich eine Verbesserung der Erfahrungen für den Karteninhaber ergibt[1]. Wenn jedoch stark angezweifelt werden muss, dass es sich um den authentischen Karteninhaber handelt, könnte die Transaktion komplett abgelehnt werden. So wird eine Autorisierungs- oder Begleichungsanforderung verhindert und die Gefahr von Betrug insgesamt beseitigt, sogar wenn der Betrüger die Authentifizierungsinformationen kennt. Bei Transaktionen, bei denen die Legitimität oder Illegitimität nicht genau bestimmt werden kann, kann es ratsam sein, eine strenge Authentifizierung des Karteninhabers vorzunehmen. Die entscheidende Idee bei der verhaltensbasierten Authentifizierung ist, mithilfe von Verhaltensmustern die Unsicherheit zu reduzieren, ob die Person, die einen Authentifizierungsversuch unternimmt, der legitime Karteninhaber ist. Dadurch wird gleichzeitig (a) der Anteil legitimer Transaktionen verringert, die durch eine sekundäre Authentifizierung beeinträchtig werden, während (b) sichergestellt wird, dass mehr Betrugsversuche eine sekundäre Authentifizierung durchlaufen und (c) mehr Betrugsversuche komplett abgelehnt werden.

Modelle für die verhaltensbasierte Authentifizierung

Die regionalen CA Risk Analytics-Modelle basieren auf Daten von regionalen Ausstellern, die ihre Daten für das CA eCommerce Consortium zur Verfügung stellen und zu „wahren Daten“ beitragen[2]. Zu diesen Daten gehören 3-D Secure-Transaktionen mit Kredit- und Kundenkarten.

Regionale Modelle bestehen aus einer Reihe unterschiedlicher Elemente. Erstens nutzen die Modelle Informationen aus der aktuellen Transaktion. Dazu zählen Datum und Uhrzeit, Betrag, Standort der Person, die den Authentifizierungsversuch für eine Transaktion unternimmt (im Fall von eCommerce der Computer oder das mobile Gerät des Karteninhabers), Händlername sowie Händler-ID und -URL, Informationen zur IP-Adresse des Geräts, Verbindungsmerkmale und Zusatzinformationen von externen Datenanbietern. Diese Informationen sind entscheidend, damit das Modell die aktuelle Transaktion analysieren kann. Sie reichen allerdings nicht aus, um das zugehörige Verhalten zu verstehen.

Zweitens nutzen die Modelle Informationen aus vorherigen Verhaltensweisen als zentrale Einheiten des aktuellen Authentifizierungsversuchs, beispielsweise Karte, Gerät oder Händler. Informationen aus vergangenen Verhaltensweisen werden zu wichtigen Faktoren bei der Betrachtung von Verhaltensmustern verarbeitet. Dazu zählen beispielsweise folgende Informationen: Welche Händler wurden besucht, die Beträge, Standorte und Geräte, die bei diesen Besuchen genutzt wurden, und welche eindeutigen Geräte wurden mit dieser Karte verwendet. Auch bei anderen zentralen Einheiten wird nach ähnlichen Mustern gesucht. Diese Protokolle werden als „zentrale Destillate“ bezeichnet, und sie werden bei jedem beobachteten Authentifizierungsversuch für eine Transaktion aktualisiert.

Drittens nutzen die Modelle komplexe Variablen wie Mini-Modelle, die die Verhaltensmuster der an der Transaktion beteiligten zentralen Einheiten isolieren und bestimmen, wie und ob die aktuelle Transaktion zu diesen Mustern passt. Diese Variablen können einfach sein und nur zur Bestimmung dienen, ob ein neues Gerät für eine bestimmte Karte verwendet wird oder mit welcher Geschwindigkeit Ausgaben über eine Karte oder ein Gerät erfolgen. Sie können aber auch komplex sein und die Tendenz eines bestimmten Karteninhabers zu einem wiederholten Einkauf sowie die Anzahl der Besuche bei diesem Händler mit den gleichen Mustern für andere Personen vergleichen.

Viertens nutzen die Modelle aus Protokolldaten erstellte Tabellen. Diese Tabellen enthalten Informationen zu vergangenen Tendenzen für legitime und betrügerische Transaktionen in den Protokolldaten, einschließlich Trend-Messdaten und Naive Bayes-Messdaten.

Schließlich werden diese unterschiedlichen Elemente in einem nicht linearen numerischen Modell verwendet, das deren unterschiedliche Vorhersagen im Hinblick auf Verhaltensanomalien und das Risiko eines illegitimen Versuchs gewichtet. Diese Modelle erfassen die nicht linearen Verhaltensweisen: wichtige Beziehungen zwischen den Variablen und die Wahrscheinlichkeit von Betrug, was keine einfache lineare Beziehung ist. Sie vergleichen Risikofaktoren mit abschwächenden Faktoren (Händler und Betrag deuten auf Betrug hin, aber diese Person hat diese Art von Transaktion schon früher auf diesem Gerät abgewickelt) und achten auf viele verschiedene Beziehungen.

Die Gewichtung dieser unterschiedlichen Faktoren wird mit einem Trainingsalgorithmus für einen großen Datensatz vergangener Transaktionen und den „wahren Daten“ vorgenommen. Derartige Modelle sind also grundsätzlich „datengesteuert“. Dadurch können diese Modelle ungewöhnliche Beziehungen ermitteln, die in Regeln nicht leicht erfasst werden können, und die beste Schätzung der Wahrscheinlichkeit anbieten, dass eine Transaktion illegitim ist.

Die Ausgabe dieser Modelle ist eine Zahl, die eine Schätzung der Wahrscheinlichkeit darstellt, dass dieser Authentifizierungsversuch *illegitim ist.* Dies ermöglicht die Bildung einer Rangreihe der Authentifizierungstransaktionen, damit unterschiedliche Aktionen durchgeführt und Prioritäten für die Aktionen vergeben werden können. Insbesondere ist so für Transaktionen basierend auf Verhaltensmustern in den Daten, die die Wahrscheinlichkeit einer Illegitimität angeben, eine „Authentifizierung im Hintergrund“ möglich, ohne den Karteninhaber zu stören.

Nicht lineares numerisches Modeling mit neuronalen Feedforward-Netzen

Unter den vielen verfügbaren numerischen Modeling-Ansätzen stellen neuronale Feedforward-Netze (Feed-Forward Neural Networks, FFNN) die ideale Kombination von Performance, Flexibilität und Machbarkeit dar.

Neuronale Feedforward-Netze sind extrem flexibel, insofern als im Eingabemerkmalsraum keine Annahmen bezüglich Struktur oder Verteilung erforderlich sind. Sie weisen auch bei sehr nicht linearen Daten eine hochmoderne Performance auf, da es sich um universelle Funktionsannäherungen handelt. Hinzu kommt, dass sie unabhängig vom Umfang oder von der Komplexität der Daten in linearer Zeit trainiert werden und in konstanter Zeit bewerten. Dadurch sind sie auch für extrem große Datensätze sehr nützlich.

Struktur neuronaler Netze

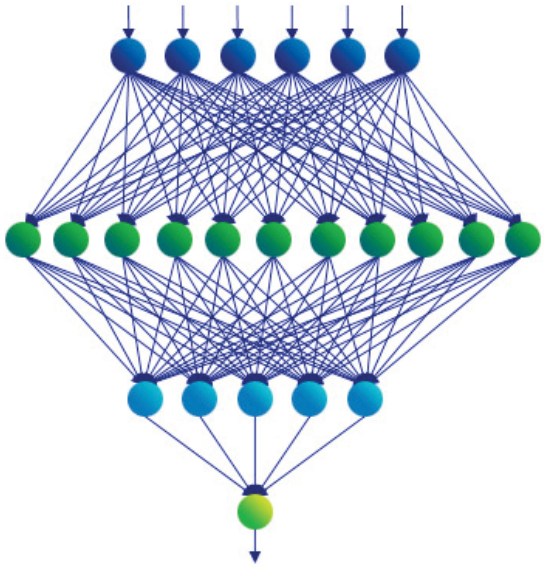
Ein FFNN ist im Wesentlichen ein gerichtetes, azyklisches, nicht lineares Signalflussdiagramm, dessen Eingabe eine numerische Darstellung der Transaktion ist, so wie sie von den oben aufgeführten Techniken erfasst wurde. Ihre Ausgabe in unserem Kontext wird als eine Ordinalmessgröße der Wahrscheinlichkeit interpretiert, das der Authentifizierungsversuch betrügerisch ist (die Bewertung).

Anschaulicher ist es, wenn Sie sich FFNNs als eine Sequenz von „Ebenen“ vorstellen, von denen jede aus einer Reihe von „Neuronen“ besteht (siehe Abbildung 2). Der als Eingabe verwendete Authentifizierungsversuch wird als erste Ebene (für die Eingabe) dargestellt, wo die Weitergabe durch das Netz beginnt. Diese Weitergabe wird durch interne Ebenen („verborgene Ebenen“) und letztlich bis zur Ausgabeebene fortgesetzt. Jede Ebene führt eine nicht lineare Transformation der Eingabe durch und gibt das Ergebnis an die nachfolgende Ebene weiter. Jede Ebene kann eine willkürliche Anzahl von Neuronen aufweisen, in unserem Kontext weist die letzte Ebene (für die Ausgabe) ein einziges Neuron auf (das die Bewertung erzeugt).

Die eigentliche Leistungsstärke von FFNNs liegt in diesen sequenziellen, nicht linearen Transformationen, die gemeinsam dazu beitragen, dass das FFNN jede Funktion der Eingabe modellieren kann.

Abbildung 2.

Beispiel für ein neuronales Feedforward-Netz (FFNN)



Abschnitt 3

Vorteile erweiterter Modelle

Modellperformance

Mit regionalen Modellen von CA können Sie die Authentifizierung für die Mehrheit der betrügerischen Transaktionen verweigern oder verstärken, und nur ein kleiner Teil der legitimen Transaktionen ist davon betroffen. Die allgemeine Performance wird in Abbildung 3 dargestellt. Das Modell maximiert die Betrugserkennung und minimiert gleichzeitig die Auswirkungen auf die Kunden. Im Diagramm wird nicht die gesamte Kurve dargestellt, der Fokus liegt auf dem operativen Bereich der Kurve.

Abbildung 3.

Die Betrugserkennung des Modells als Funktion des Prozentsatzes aller vom Modell gekennzeichneten Transaktionen. Im Diagramm wird nur ein Teil der Grundgesamtheit dargestellt, der Fokus liegt auf dem operativen Bereich der Kurve.

Bewertungen und Regeln von Modellen

Regeln können sehr gut für präzise, bekannte Betrugsindikatoren genutzt werden. Sie lassen sich schnell implementieren und sind leicht verständlich. Sie sind jedoch nicht datengesteuert und daher auf das Wissen beschränkt, das der Verfasser der Regel im Hinblick auf mögliche Signale für Betrug hat. Regeln können komplexe Verhaltensweisen nicht einfach erfassen und sind nicht dazu geeignet, mehrere Risiken in einer Entscheidung zu kombinieren. Und schließlich können sie keine Rangreihe der Transaktionen bilden, um eine Anpassung der Ablehnung, der sekundären Authentifizierung und der Fallgrößen zuzulassen.

Modelle erfassen mithilfe von durchdachten Variablen komplexe Muster. Die Variablen basieren auf der aktuellen Transaktion und auf den zentralen Destillaten (wichtigen Informationen aus früheren Transaktionen zu zentralen Kennungen in Transaktionen, die heruntergebrochen wurden). Mit nicht linearen und linearen Variablen sowie bewährten Trainingstechniken ermöglichen die Modelle eine Gewichtung verschiedener Faktoren über einen datengesteuerten Ansatz. Sie erzeugen eine Rangreihe der Transaktionen, die auf der Wahrscheinlichkeit von Betrug basiert. Allerdings werden Modelle nicht selbst aktiv, sondern müssen durch Regeln ergänzt werden.

Gemeinsamer Einsatz von Regeln und Modellen

Im Hinblick auf die unterschiedlichen Stärken von Modellen und Regeln empfiehlt es sich, beide gemeinsam zu nutzen. Nutzen Sie zuerst ein starkes Modell, um zwischen betrügerischen und legitimen Transaktionen zu unterscheiden, und erstellen Sie dann mit einer Bewertung eine Rangreihe der Transaktionen. Schreiben Sie anschließend Regeln, in denen diese Bewertung auf verschiedene Arten genutzt wird: (i) Eine hohe Bewertung weist auf eine große Wahrscheinlichkeit von Betrug hin und sollte verwendet werden, um Maßnahmen zu ergreifen und den Bewertungsschwellenwert anzupassen, sodass der von der Institution gewünschte Umfang von Betrug erreicht wird. (ii) Eine niedrige Bewertung kann in Verbindung mit Regeln für Flash-Fraud und anderen Regeln verwendet werden und die sehr wahrscheinlich legitimen Transaktionen herausfiltern, sodass die Regeln auf einen umfangreicheren Datenpool zugreifen können. Und schließlich gibt es von der Institution implementierte Richtlinienregeln, die von der Betrugswahrscheinlichkeit unabhängig sind. Sie erfordern unabhängig von der Betrugswahrscheinlichkeit möglicherweise eine sekundäre Authentifizierung für neue Geräte.

Abschnitt 4

Schlussfolgerung

Der Einsatz einer verhaltensbasierten Authentifizierung, um die Transaktionen zu bestimmen, bei denen eine Authentifizierung oder Ablehnung erforderlich ist, ist entscheidend, um z. B. Reibungspunkte bei Kunden zu verringern und besser zu gewährleisten, dass die Transaktion legitim ist. Regeln sind eine wichtige Komponente für diese risiko- und verhaltensbasierte Authentifizierung. Sie weisen jedoch einige Einschränkungen auf. Wenn durchdachte verhaltensbasierte Modelle hinzugefügt werden und die Anwendung risikobasierter Regeln vorgeben, kann der Einfluss auf illegitime Versuche beträchtlich erhöht werden. Gleichzeitig werden die Auswirkungen auf legitime Kunden verringert, sodass die Erfahrungen für den Karteninhaber optimiert und die Verluste für den Aussteller verringert werden.

Abschnitt 5

Informationen über die Autoren

Paul Dulany arbeitet seit 14 Jahren im Bereich Advanced Analytics und Data Science. Er kam 2013 zu CA Technologies und war maßgeblich an der Entwicklung der analytischen Modeling-Infrastruktur und dem ersten vom CA Data Science-Team produzierten Modell beteiligt. Vor CA Technologies war er für mehr als acht Jahre beim SAS Institute beschäftigt. Dort war er in dem Team, das die ersten Modelle für die SAS Enterprise Fraud Management-Lösung entwickelt hat. Außerdem hat er die Entwicklung der ersten Modelle für Kundenkarten geleitet und viele neue Techniken entwickelt. Vor SAS war Paul Dulany für mehr als fünf Jahre bei HNC und Fair Isaac. Dort war er als Wissenschaftler und später als Leiter des Fraud Predictor Modeling Teams tätig und hat eine Reihe von Modellen für Falcon-Zahlungskarten entwickelt und in anderen Bereichen gearbeitet. Aus seiner Zeit bei HNC und SAS besitzt Paul Dulany Patente, und er hat außerdem einen Ph.D. in theoretischer Physik.

Hongrui Gong verfügt über umfassende Erfahrungen im Bereich Advanced Analytics und Data Science. Er kam im April 2013 zu CA Technologies und hat entscheidend am Aufbau einer Modeling-Infrastruktur und an der Entwicklung von Modellen für 3-D Secure-Produkte mitgewirkt. Bevor er zu CA kam, hat er für mehr als 15 Jahre bei namhaften Analyseunternehmen (SAS, FICO und HNC) gearbeitet. Dort hat er Modelle für verschiedene Produkte entwickelt: Betrugserkennung bei Zahlungskarten, Erkennung von Versicherungsbetrug, Identifizierung von Steuerhinterziehung für Regierungsbehörden, Schutz vor Geldwäsche, Vorhersage von Kreditausfällen, Risikomanagement bei

Vermittlungsgeschäften und Risikobewertung bei Krediten für Aktiengesellschaften und private Unternehmen. Hongrui Gong hat einen Ph.D. im Bereich numerische Strömungsmechanik. Er verbrachte vier Jahre im Los Alamos National Laboratory und hat zu theoretischem Modeling und Computersimulationen turbulenter Strömungen geforscht. Er besitzt eine Reihe von Patenten aus seiner vorherigen Arbeit.

Kannan Shah arbeitet seit sechs Jahren im Bereich Advanced Analytics und Data Science. Er kam 2013 zu CA Technologies und war an der Entwicklung der analytischen Modeling-Infrastruktur und dem ersten vom CA Data Science-Team produzierten Modell beteiligt. Bevor er zu CA Technologies kam, war er Senior Staff Scientist beim SAS Institute, wo er für die SAS Enterprise Fraud Management-Lösung statistische Modelle und Techniken entwickelt und im Kundensupport gearbeitet hat. Er war an der Entwicklung von Modellen für die Betrugserkennung bei Zahlungskarten und ACH-Transaktionen sowie Überweisungen beteiligt, die in den USA, Großbritannien, Mexiko und im Asien-Pazifik-Raum eingesetzt werden. Kannan Shah besitzt eine Reihe von Patenten aus seiner Zeit bei SAS. Er hat einen M.Sc.-Abschluss in Elektrotechnik von der Drexel University in Philadelphia. Zu seinen Studienschwerpunkten gehörten Erkennung und Schätzung, stochastische Signalverarbeitung, Maschinenintelligenz, statistische Mustererkennung, neuronale Netze, Informationstheorie, Spektralanalysen höherer Ordnung sowie Design und Komplexität von Algorithmen.

Kontaktieren Sie CA Technologies unter ca.com/de

CA Technologies (NASDAQ: CA) entwickelt Software, die Unternehmen bei der Umstellung auf die Application Economy unterstützt. Software steht im Mittelpunkt jedes Unternehmens in allen Branchen. Von der Planung über die Entwicklung bis zu Management und Security – CA Technologies arbeitet weltweit mit Unternehmen zusammen, um die Art, wie wir leben, Transaktionen durchführen und kommunizieren, mit zu verändern, ganz gleich, ob in mobilen, privaten und öffentlichen Cloud-Umgebungen oder in verteilten Systemen und Mainframe-Umgebungen. Weitere Informationen finden Sie unter **ca.com/de**.

1 In Regionen, in denen Karteninhaber intensiv darüber informiert wurden, auf 3-D Secure-Zeichen zu achten, kann es für den Karteninhaber beruhigend sein, wenn in einem zusätzlichen Fenster darauf hingewiesen wird, dass diese Transaktion mit 3-D Secure geschützt ist.

2 Der Begriff „wahre Daten" bezieht sich auf Transaktions- und Karteninformationen, um die Transaktionen zu identifizieren, die im Authentifizierungsprozess beendet werden sollen.

CS200_94860_1014