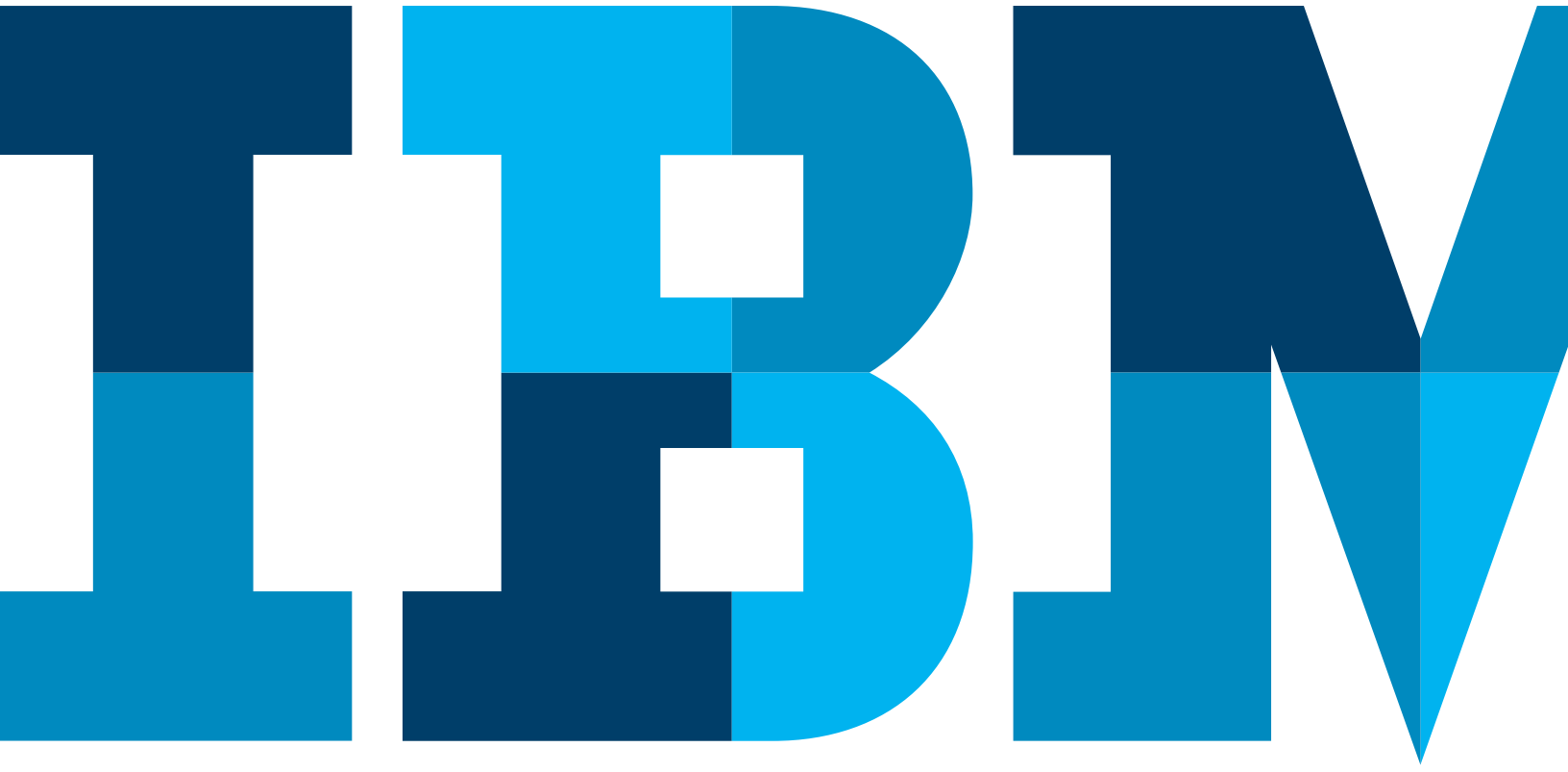
IBM Tealeaf solutions and fraud

The value of visibility into the forensic environment



IBM

Contents

By Robert Wenig, Tealeaf CTO, IBM Software Group, ExperienceOne

It used to be that I could not say the "F" word (fraud), but now that it is front and center on our website as a value proposition, my fingers are allowed to type freely.

Seriously, I have had a lot of interesting conversations with our customers and prospects about how IBM Tealeaf solutions can help with fraud. I would like to share what I have learned and solicit your feedback.

Please keep in mind that IBM Tealeaf solutions are not fraud solutions. We acquire our data passively (i.e. out of band through a network tap or span port)—the value of IBM Tealeaf solutions to solving the fraud problem comes from providing insight.

Value proposition

IBM Tealeaf solutions have provided leading organizations with unprecedented visibility into their customers' online experiences by capturing each customer's interaction, each time—creating a 360-degree view that enables companies to answer many of the compelling questions asked by online businesses.

The insights gleaned from using IBM Tealeaf solutions have traditionally been utilized to help with:

- Customer conversion and retention
- Application problems
- Web and mobile app usability
- Customer dispute resolution

IBM Tealeaf solutions are different from an IDS (Intrusion Detection Systems) or web analytic tools in that we acquire and persist the whole data stream. IDS systems tend to decimate (i.e. keep only the snippets that they need) in real time, while web analytic tools tend to get their insight from pre-configured page tags. IBM Tealeaf solutions acquire and keep the whole HTTP Request and HTTP Response.

Utilizing this comprehensive data set, we can:

- **Replay**—IBM Tealeaf solutions enable you to see your customers' actual on-line experiences, analyze their motivations and, ultimately, gain insight as to why abandonment or other site actions occur.
- **Search** (forensic)—In addition to normal "free text" search, IBM Tealeaf solutions can search on the metadata of a session—i.e. time, number of pages, or the value of a particular form field. This is done without the need for

metadata editing or setup. So, when a customer reports a problem, you can find their session and then assess impact by finding similar sessions.

- **Insight**—The Events function found in IBM Tealeaf solutions can power embedded or external dashboards, Key Performance Indicators, scorecards and more.
- **Export**—IBM Tealeaf solutions support a number of methods to programmatically access the data. These include:
  - Real time via Event Bus—The ability to send data/insight out of the IBM Tealeaf system in real time via a TCP/IP connection.
  - Constraint Based Search Extraction—Batch mode extraction to a flat file or relational store.
  - Export of Session with IBM Tealeaf cxVerify—Case Management. Encapsulate a session into a neutral file format (PDF) along with metadata. This allows for indefinite persistence of sessions of interest. Also allows for integration with document management systems.
  - IBM® Tealeaf® cxReveal integration—Allows third-party applications to request a replay of a session stored by IBM Tealeaf solutions. For example, 41st parameter (anti-fraud solution) initiates a replay request via a common key or cookie value. Many of our customers have anti-fraud systems. They are rules driven, and they make suggestions as to which orders to investigate further. The CSR (i.e. Tealeaf cxReveal) integration allows a person to quickly examine a session and see which rule(s) caused the session to be kicked out for further examination.

How to leverage IBM Tealeaf solutions to help fight fraud

There are many aspects to combating fraud, spanning multiple disciplines and organizational boundaries. Again, since IBM Tealeaf solutions passively monitor network activity—most of their value comes from insights gleaned from their use—in no way are they a turnkey fraud solution.

With IBM Tealeaf solutions, we can:

- **Detect**—Become aware of fraudulent activity—either in real time or post mortem.
- **Stop**—Block access to the site—or prevent the goods from leaving (time-delayed).
- **Research/investigate**—Social networks (pivot)—here is an area where IBM Tealeaf solutions shine. Because we capture the whole stream of traffic we can facilitate forensic discovery. Other traffic activities investigated for fraud include:
  - Same IP address
  - Same account number
  - Same e-mail
  - Same cell phone or address
  - Same item
  - Same credit card number
  - And more (discussed below)
- **Report impact**—Understand what the true loss may have been. Which accounts have been breached? What Personally Identifiable Information (PII) was displayed—and to whom? Many times fraudsters do things that are not transactional in nature—i.e. no data changes on the back end. So, what is the harm? If PII was obtained—even in a read-only form—this is very dangerous because it may be used in a subsequent foray.

- **Remedial action**—When an attack succeeds, you must notify all affected parties. If you do not know what information was disclosed—then you have to notify your entire user base—which can be a very public, embarrassing, and expensive proposition (i.e. each letter costs one dollar, credit protection services costs $100 per user, loss of reputation is priceless). Since IBM Tealeaf solutions keep a constant record of what is happening on your site, the scope of remediation can be narrowed down to the truly affected parties. For example:
  - At one larger multichannel retailer, one of the "fraud signatures" was people who placed an order and then repeatedly checked order status within the first day to see whether or not the fraud team allowed the order. This is now a simple sequence query.
  - One hit (or non productive) session analysis by Referrer or by IP—again a simple query against the Visitor DataBase (VDB). The data is already in the datamart—so we are just one SQL query away.

Deploying IBM Tealeaf solutions to help prevent fraud: Examples

Omni-channel retailer

This omni-channel retailer's loss prevention team is made up of eight members that regularly look at orders prior to shipping in order to determine and react to orders that have "risk".

The loss prevention team has basically 24 hours after an order is placed to second check the validity of the order. The online order has been accepted by the credit card company (Discover, Amex, MC, Visa)—however, the merchant is at risk for any misuse of the card.

So, they review orders. Perhaps, for electronics greater than $300, they manually look at the order; look up the address for past problems, etc. They decide to allow the order, cancel the order, or require more verification (i.e. call the customer or the credit card company) and in turn carry responsibility for authentication.

IBM Tealeaf solutions add visibility in this discovery process because they allow searching across dimensions, by product, by credit card number (even if hashed), by address, by phone number or by e-mail address. The in-house system does not allow for this. In addition, we can event on "tried more than one credit card", or "attempted credit card validation multiple times" (i.e. trying to get an address which the credit card processor will allow tied to a number), etc.

This retailer liked our ease of deployment and the fact that we are passive.

A leading airline

This airline identified one of the most common fraud practices—users entering different credit card numbers multiple times and then having a successful purchase after multiple failures.

Other fraudulent activities involved purchasing tickets for same day travel that the airline team could not detect until post-mortem.

With IBM Tealeaf solutions, the fraud detection team can investigate for fraudulent activities in real time. The team is quickly alerted to bad e-mail addresses and credit cards, and can investigate further by drilling down and searching the users's e-mails, IP and names. These capabilities have helped the team to decrease fraudulent activities on the airline's site.

A top retailer

When talking to this top retailer's loss prevention team, they identified multiple fraud indicators and are using IBM Tealeaf solutions to bolster their case. By using IBM Tealeaf solutions to monitor for common indications of fraud, they have been able to identify Eastern European fraud rings, track IP addresses (multiple IP addresses per session or employee using customer's gift card, for example) and identify "rejected codes" such as rejected credit card numbers and zip codes (both indications of possible fraud).

Once the prevention loss team discovers fraud, they can drill down by phone number, zip code, IP address and/or mailing address to find other cases that they did not catch previously. Other fraud indicators the team also monitors are the number of orders per session and users who check their order status frequently from different browsers and locations.

The prevention loss team then exports the saved recorded sessions from IBM Tealeaf solutions to share with law enforcement agencies including the FBI, Secret Service, Internet Crime Complaint Center (IC3), and local law enforcement.

Additional fraud detection examples from multiple customers

- Process fraud—sign up for insurance and process a claim on the same session.
- Process fraud—purchase order online and check repeatedly to see if loss prevention approves the order.
- Process fraud—loan signer and co-signer in same web session (should be two distinct sessions, different IP's, etc).
- Process fraud—attempt to reset password with different IP addresses on the same account number.
- Electronic cash—using a script generator to attempt and validate a sequence of digits. A correct set of numbers is equivalent to cash—this is like dialing for dollars.
- Credit card application—apply for credit card after getting rejected and change the business name in the same session.
- Ratios changing in KPIs—order ratio, rejected credit card ratio, logon failures ratio, etc - all indicate a problem.
- Data mining—given the rich and comprehensive nature of the data acquired and persisted by IBM Tealeaf solutions the information gleaned from them is a data miner's dream. Suppose that in the course of a day, 100 incidents of fraud are discovered. Most likely, the report of fraud will come from the credit card customer or via the credit card company as a chargeback. Using IBM Tealeaf solutions, the affected sessions can be found. In addition to normal "Replay", the underlying facts of the session (time, IP, browser type, other patterns of behavior) can be extracted and presented to a 3rd party data mining tool. The tool can then look for correlations between fraudulent sessions that may have escaped the naked eye. The output can then be used to identify fraudulent activities that have already happened, but not yet reported or, more importantly, to help predict future fraudulent use.
- Data protection—Most customers configure IBM Tealeaf solutions to block (i.e. permanently destroy) sensitive data. This includes credit card numbers, passwords, etc. Thus if you want to find a session by credit card number, you may be out of luck. Or, if you want to see if people are trying the same password (on failed login attempts) across multiple logins, etc.

In addition to supporting destruction of sensitive data, IBM Tealeaf solutions can also MD5 (Message-Digest Algorithm) hash a value. This does a one way translation of a value into a 32 byte string, which cannot be reversed. So, if you wanted to search by credit-card number, you could MD5 hash the value which destroys the utility value as a credit card number. If you want to search for this value, you enter the customer supplied number and click the "hash button". By using MD5 to hash value, users of IBM Tealeaf solutions can:

- Audit—who accessed the data and when? Initially, I thought that this was for internal applications only, i.e. did a CSR look up the account activity of John Doe, etc.—however as the lines between intranets and internets blur, this is much, much more. A large bank may extend a wholesale banking portal to a multi-national customer. The multi-national customer wants to know what banking information did each employee look at.
- Geolocation analysis (we can transform IP to city/state—do we report/compare—measure distance as compared to known—or via application form)—compare billing zip code to IP address, etc., including:
  - By business process
  - By password reset
  - New account opening
  - By sale

Sometimes it is also useful to see what happens after a key business process, i.e. wire transfer request after password reset, may be a red-flag.

Network affect

IBM Tealeaf solutions are widely deployed within financial services, retail, travel, telco and other key verticals. All of our customers are under pressure to deal with fraudulent activities. Fraud is a societal problem, not a company or industry challenge. It is highly unlikely that the bad guys will target just one bank, or one online retailer—they will attack many.

Summary

Fraudulent activity is clearly getting more and more sophisticated. E-commerce companies need visiblity to fight against fraudulent activies happening on their websites.

When I ride my bike, I wear a helmet. When I drive a car, I wear a seat belt. When I run a website, I use IBM Tealeaf solutions.

About IBM ExperienceOne

IBM ExperienceOne helps you attract, delight and grow the loyalty of customers by enriching the ways you engage each of them. IBM ExperienceOne provides a set of integrated customer engagement solutions that empower marketing, merchandising, commerce and customer service teams to identify the customers and moments that matter most, and to rapidly apply those insights to develop and deliver personally rewarding brand experiences.

IBM ExperienceOne ignites innovation by leveraging patterns of success from more than 8,000 client engagements, original industry research, and products consistently recognized as industry leaders in major analyst reports.

IBM ExperienceOne solutions are delivered in cloud, on premises, and in hybrid options.

For more information

To learn more about IBM ExperienceOne, please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/experienceone.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
November 2014

Please Recycle

ZZW03244-USEN-03