IBM Tealeaf solutions deployment architecture and security model

Robust set of security features to meet enterprise privacy and security requirements

Highlights

- Non-intrusive and security-rich data collection with encrypted data transport
- Data encryption, destruction and filtering designed to protect sensitive data
- Password protected and encrypted configuration files to protect critical configuration options
- Data segmentation to support session-level segmentation by user group
- Data routing and data filtering settings are accessed and modified only by authorized personnel

IBM Tealeaf solutions provide unprecedented visibility into a customer's online experience. At the same time, the Tealeaf platform provides the protections necessary to maintain the privacy of the information it monitors. To meet the requirements of simultaneously managing mission-critical web applications and complying with enterprise security requirements, IBM Tealeaf solutions include a robust set of security features designed to provide security-enhanced data capture, transport, storage and access. As a result, IBM Tealeaf solutions have satisfactorily passed security audits conducted by our customers, including major national and international financial institutions.

The Tealeaf platform enables businesses to dramatically improve conversion rates while significantly reducing support costs, by helping them to quickly detect, analyze and respond to problems blocking customers from successfully completing online transactions. It does this by delivering real-time, browser-level visibility into each customer's online experience. To provide this level of visibility, IBM Tealeaf solutions capture what customers are doing and seeing in real time by passively recording the HTTP(S) request and response stream.

In turn, this data enables real-time detection of application failures and issues preventing real users from completing transactions. Users of IBM Tealeaf solutions can quickly conduct a business impact evaluation of a problem by recreating it through a visual replay of a saved copy of the user session to assess the nature of the problem with full context such as user actions and transaction values. IBM Tealeaf solutions also identify how many other users were impacted by similar problems and enable users to isolate and diagnose the causal factors of the problem by correlating session attributes within and across effected user sessions.

Exactly which information IBM Tealeaf solutions capture, encrypt or destroy and whether specific information is viewable by the various classes of users is configurable. To aid security evaluations, this document describes the general deployment architecture and specific security features of IBM Tealeaf solutions including:

- Non-intrusive and security-rich data collection
- Encrypted data transport
- Data encryption, destruction and filtering to protect sensitive data
- Password protected and encrypted configuration files to protect critical configuration options
- Access controls with Windows Domain Authentication
- Data segmentation to support session-level segmentation by user group
- Access and change audit

IBM Tealeaf solutions: deployment architecture overview

IBM Tealeaf solutions are distributed into three core components: a) Passive Capture, b) the Tealeaf Processing environment and c) the IBM Tealeaf Portal and RealiTea Viewer end-user clients.

- **Passive Capture**: Passive Capture records the HTTP(S) request and response data using a Passive Capture Server (PCS)—which passively "sniffs" leveraging an existing spanning port or network tap. The PCS asynchronously records a copy of the HTTP(S) request and response and transports it to the Tealeaf Processing environment for processing (see Non-intrusive and security-rich data collection).
- **Tealeaf Processing environment:** The Tealeaf Processing environment is a highly scalable, real-time, distributed platform that processes, analyzes, indexes and archives the recorded data. It also serves as the platform for the IBM Tealeaf Portal and RealiTea Viewer clients and the IBM Tealeaf family of products.

Typically deployed behind the DMZ in a trusted network segment, the Tealeaf Processing environment operates on the Windows 2008 and 2012 (64-bit) Server or Advanced Server platform.

The Processing Server receives data in real time from the PCS on a configurable port (typically port 1966) in our proprietary data format packaged in TCP/IP. When received, the data is streamed through a pipeline consisting of multiple session agents that perform specific filtering, manipulation and routing functions. Among those functions include the decryption and filtering of sensitive information (see Sensitive data encryption, destruction and filtering). The master configuration file for the data transport pipeline can be optionally password- protected and encrypted.

From the pipeline, the data is analyzed, evaluated, indexed and archived. These functions are conducted by the Short-Term Canister, Indexer, Long-Term Canister and Archive Manager components. Data access requests, such as queries from the IBM Tealeaf Portal or RealiTea Viewer, to these components are brokered and administered by the Search Server web service. The Search Server web service is a middle-tier transaction broker that services querying, security, data collection and administrative functions (e.g., collecting health metrics, publishing RealiTea Viewer profiles) for the IBM Tealeaf Portal and RealiTea Viewer clients.

Using Windows Domain Authentication, the Search Server grants or denies access by authenticating the request against the user permissions defined using Windows NT Authentication (see Data segmentation: see Access controls using Windows Domain Authentication).

- **IBM Tealeaf Portal and RealiTea Viewer end-user clients**: The IBM Tealeaf Portal is a real-time, web-based console that provides a centralized workspace for the production support team to identify, size and diagnose issues impacting business-critical web applications, as well as a tool for administrators to manage the overall health of IBM Tealeaf solutions. It offers a real-time view of user activity, searching capabilities and reporting functionality to provide rapid awareness and problem resolution.

  The RealiTea Viewer is a win32 client used by the production support team and other users of IBM Tealeaf solutions to recreate problems or other issues by visually replaying the real user's interaction with the web application. The user session is replayed step-by-step, as it was recorded at the time the real end-user conducted the session. In addition, the RealiTea Viewer also provides advanced search and correlation functionality for advanced causal factor isolation and problem diagnosis.

  The IBM Tealeaf Portal web application is served from the Tealeaf Server. The IBM Tealeaf Portal can be served from over HTTP (port 80) or HTTPS (port 443). End-user access to the IBM Tealeaf Portal is controlled via its native authentication system or by using Windows NT Authentication to administer groups and users on the Tealeaf Server machine. Database access via the RealiTea Viewer can also be controlled using Windows NT Authentication (see Access controls using Windows Domain Authentication). In addition, data query, end-user and administrative actions conducted via the IBM Tealeaf Portal and Viewer clients is logged to enable auditing of which end-user requested and accessed what data (see Access and change auditing).

IBM Tealeaf solutions: security features

Non-intrusive and security-rich data collection

The PCS passively "sniffs" TCP/IP packets from the network leveraging an existing spanning port or network tap and is not an inline device.

Tealeaf Passive Capture runs on RHEL 5, and RHEL 6 (starting with PCA build 3502), and SUSE 11. It leverages proprietary software to collect the TCP/IP packets, reassemble the packets into the HTTP(S) request and response objects, apply configurable filtering rules (e.g. delete HTTP(S) image objects) and transport assembled HTTP(S) request and response objects to the Tealeaf Server environment (see Encrypted data transport).

To collect data, the PCS is connected to either a spanning port or network tap. For receiving and sending data, the PCS has two listening ports and one sending port, respectively. Neither of the listening ports have a published IP address.

To decrypt SSL, the PCS uses a copy of the SSL private key certificate to decrypt HTTPS traffic out-of-band. Private keys are encrypted using OpenSSL library's 3DES encryption algorithm and stored in our proprietary file format (.ptl).

In addition, a machine-specific hash ID is included to prevent the encrypted key file from working on other machines, helping to eliminate the possibility of the encrypted file from being hijacked and used on a different machine to decrypt SSL traffic. In addition, it also supports nCipher's nShield Hardware Security Module (HSM) for private key management.

The PCS can be administered either using a password protected web-based console accessed over HTTPS (port 8443) or directly by accessing the PCS over SSH (default port is 22, but can be configured by administrator).

Encrypted data transport

The data stream from the PCS can be encrypted during transport to the Tealeaf Server environment. Using OpenSSL, the data is encrypted using a 2048-bit private key.

On the receiving Tealeaf Server machine, the data stream is decrypted by a decryption agent using a provided self-signed SSL certificate. Optionally, the self-signed certificate can be replaced with a customer-issued SSL certificate.

Sensitive data encryption, destruction and filtering

Companies have several powerful choices for protecting or removing sensitive or private data. This helps to ensure that certain customer data is appropriately protected or destroyed—so that it is neither stored in the clear, nor capable of reaching unauthorized personnel.

- **Global data filtering**: IBM Tealeaf solutions can globally destroy sensitive data from the data stream to help prevent unauthorized users from accessing and exploiting sensitive data. Data selected for destruction is deleted in memory and not persisted in the Tealeaf Server. For example, data such as user passwords, social security numbers, account numbers or other data determined as sensitive that is being passed as an attribute in the HTTP(S) request or appearing in the HTTP(S) response page can be completely or partially destroyed.
- **Encryption of sensitive data**: IBM Tealeaf solutions possess a robust set of rules to catch and encrypt sensitive data at the point of capture. For example a credit card number or SSN can be encrypted using the 3DES or AES algorithm.This helps to ensure that even if these fields of data are preserved in the session, it will not be stored in clear-text on the Tealeaf Server.
- **Roles-based data blocking**: IBM Tealeaf solutions also support roles-based data blocking so recorded customer sessions that include sensitive customer information can be distributed while retaining the confidence that only the right people see the data for which they are entitled.

Password protected and encrypted configuration files

Select Tealeaf configuration files can be optionally password protected and stored in an encrypted format to help ensure configuration files that control data routing and data filtering settings are accessed and modified only by authorized personnel.

This is accomplished in two ways. First, the file is encrypted using 3DES or AES and a key known only to the IBM Tealeaf software components. Secondly, a username and password, assigned by an authorized person, is used to create an SHA1 hash value, which is written to disk as part of the encrypted configuration file. When the file is accessed for editing, the user is prompted for the username and password, which is then used to create an SHA1 hash value that is compared against the hash value in the file. Access is only granted if the resulting hash value matches the value in the file.

Once a configuration file is encrypted, it may only be viewed and/or edited using the Tealeaf Management System (TMS) via the IBM Tealeaf Portal. User access and changes made to the configuration file are logged by TMS, along with the user ID of the user who made the change. Access to TMS is controlled by the IBM Tealeaf Portal's user access control and authentication.

The IBM Tealeaf software is still able to access the configuration files because each component identifies itself as a privileged application when loading, and the file is automatically decrypted in memory and made available to the software.

Access controls using Windows Domain Authentication

As mentioned above, IBM Tealeaf solutions include two client applications: a) the web-based IBM Tealeaf Portal and b) the win32 RealiTea Viewer client.

The IBM Tealeaf Portal features two-tier data access controls. First, access is password protected using Windows Domain Authentication. Each user is assigned a group, which can be the same groups defined in the Windows Domain.

For each group, specific navigation directories can be enabled or disabled, governing access to functionality based per role—for example, only allowing administrative users to access the administrative functions accessible via the IBM Tealeaf Portal.

Second, session queries submitted to the Tealeaf Server are brokered by the Search Server and must be successfully authenticated against the Windows Domain credentials (when this authentication is enabled) before it is processed and results returned.

While the RealiTea Viewer is primarily used for visually replaying recorded real-user sessions, it can also be used to query the index of archived sessions. Access to the database via the RealiTea Viewer is managed in a similar multi-tiered access model. First, this is achieved by only installing the RealiTea Viewer client on the desktops or workstations of authorized and licensed users. Second, (like the IBM Tealeaf Portal) a query request submitted by the RealiTea Viewer is brokered by the Search Server and must be authenticated against the Windows Domain credentials before it is processed.

Data segmentation

In scenarios where a single Tealeaf Server environment is supporting multiple applications and there is a requirement to limit specified users to data for a specific application(s), IBM Tealeaf solutions support the ability to segment data and define user access permissions at the session level by leveraging Windows NT Authentication. In other words, a specific business group can be limited to accessing only a specific set of user sessions and so forth.

Session-level permissions are enabled using IBM Tealeaf Events. First, an event is configured to define the application type associated with the user session (e.g., Application A, Application B, etc.) Then, for the application event itself, an attribute is set to define which Windows NT user groups have access privileges to the sessions. When a query is submitted by either the IBM Tealeaf Portal or RealiTea Viewer client, the Search Server web service authenticates the client request against the defined user group permissions for the matching search results and denies or permits the query results request accordingly.

Access and change auditing

IBM Tealeaf solutions log end-user and administrative activities to provide an auditable record of activities for internal audits and to manage change control. These include:

- **Session query and access**: The Search Server component logs each session query and access actions from both the IBM Tealeaf Portal and RealiTea Viewer clients. Log data includes date, user id, query parameters, number of results and id of the session that was retrieved.
- **End-user and administrator IBM Tealeaf Portal usage**: End-user and administrative activities in the IBM Tealeaf Portal are logged including date, user id, action and status of the action.
- **Configuration files changes**: For the select configuration files, the date, userid and changes are logged.

IBM Tealeaf Event changes: For actions taken on an event definition (e.g. create, modify, delete), the Event Editor logs date, user id and change information.

For more information, please contact your IBM Tealeaf Support Representative.

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
October 2014

Please Recycle

ZZS03170-USEN-01