LP Mobile Security Overview

Document version: 2.1

October 2015

Data Sheet

LIVEPERSON

Introduction

LivePerson's mobile engagement solutions provide a unique visitor experience through seamless integration with native iOS and Android applications, as well as with iOS and Android optimized mobile sites. The solution is fully integrated within existing LivePerson deployments, avoiding any additional operational overhead.

As a leading SaaS provider with more than 15 years of experience in the industry, LivePerson understands that working in cloud-based environments may raise security concerns. We have addressed this key issue within our core security offering, in order to enable our customers to trust us with their most confidential data.

How does it work?

LP Mobile can be implemented in two different ways:

1. Embed the LP Mobile SDK in your native Mobile Application.
2. Embed the LP Mobile Tag on your mobile website.

In both scenarios, the communication between visitor and agent is established over the same secure method (HTTPS).

High-Level Structure

The diagram below provides an overview of the high-level structure:

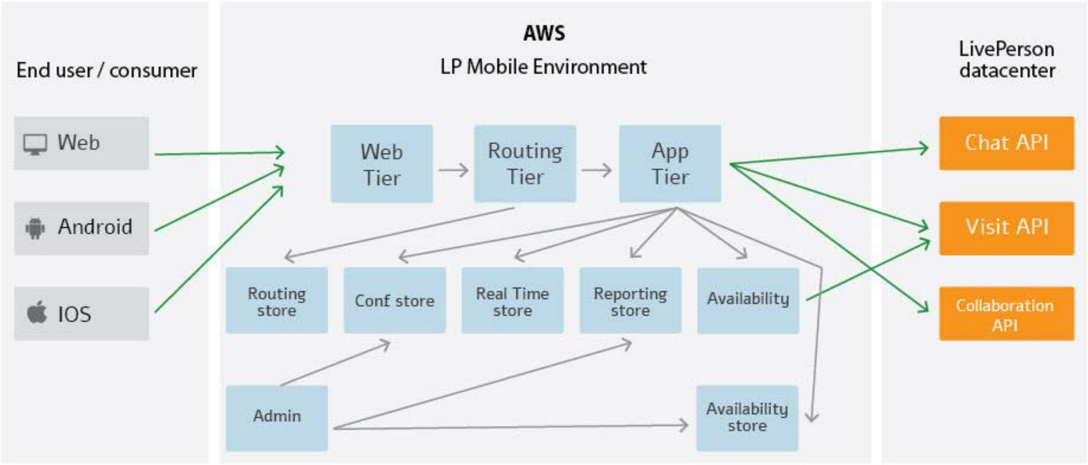

Figure 1: High-level architecture and data-flow

***Note:** Green arrows indicate encrypted communication; gray arrows indicate non-encrypted communication.*

System Components

Web Tier: Used as a reverse proxy and for static content serving, SSL termination, and load balancing.

Routing Tier: API implementation and validation, load balancer to app tier, and maintain stickiness to the assigned app instance once a visit session has started.

App Tier: The translation layer between the LP Mobile domain model and LivePerson's domain model. Implements some features on top of LP capabilities, for example, photo upload, start typing before the agent joins the chat, and more.

Availability: Fetches the agent's availability, for example, online, busy or offline, and stores it in the availability store.

Admin: Backend configuration of apps. For internal use only.

Routing Store: Stores the mapping between a visit session and an app instance.

Conf. Store: Stores the apps configuration.

Real Time Store: Stores real-time data such as mapping between mobile visit and visit session in LivePerson. No sensitive data is stored.

Reporting Store: Stores metrics such as number of visits and chats per app. These metrics are displayed in the Admin Console and are for internal use only.

Availability Store: Stores the agent's availability, for example online, busy or offline, for each skill for every site.

Use of Amazon infrastructure and services

LivePerson uses the following Amazon infrastructure and services:

Amazon CDN (Cloudfront)	LivePerson uses Amazon Cloudfront for edge hosting of static files. No customer data is stored on or transferred through this service, and only the liveperson-mobile.js and other static supporting files, for example CSS and images, are hosted by the Amazon Cloudfront CDN.
Amazon S3	The static files that are delivered by the Cloudfront CDN are stored on an Amazon S3 storage bucket that was provisioned for that purpose alone. It does not serve as storage for other components.
Amazon EC2	LivePerson uses Amazon EC2 to host the LP Mobile application components that communicate with the native LivePerson platform infrastructure. The communication is based on LivePerson standard APIs and data is only processed in EC2 server memory (no storage to disk).

Data Location

Within AWS: LP Mobile operations and data processing is based in an Amazon Web Services data center that is located in N. Virginia, USA. The data is not distributed to other Amazon data centers, regions or locations.

LivePerson Data Centers: After the data has been processed in the Amazon environment, it is transferred to the LivePerson data center where the customer account was originally implemented and installed.

Encryption of Data in Transit

Communication over the Internet is established over 256bit encrypted channel using TLS 1.1 and 1.2. Certificates are installed on an NGNIX powered web-servers. Keys are stored in a secure, private repository, and are accessible to the minimal number of operational staff members, with two factor authentication.

Protecting Data at Rest

Avoiding storage of chat transcripts within the LP Mobile environment on Amazon is a key element of the security design. Such data is only processed and transferred in real time to LivePerson's data center. LivePerson customers can use the following data protection controls In order to protect the data at rest within LivePerson's data centers.

Encryption of data at rest

Customers may opt to encrypt data at rest using 192 AES encryption once data is stored in the LivePerson data centers. If such control is enabled, as soon as the chat session concludes, the Application server encrypts the data, using unique keys that were provisioned for each customer, prior to storage. Each customer is assigned with a unique encryption key, and, additionally, each chat session is encrypted with a unique key for that session (for example, 2 chat sessions of the same customer will be encrypted with 2 different keys).

Masking of data at rest

LivePerson's platform include an optional feature that allows customers to define specific sensitive data patterns and remove them from the chat transcripts prior to storing the transcript in the data repositories. The masking is based on a RegEx mechanism that identifies the sensitive pattern as configured by the customer, and replaces them with xxxx or *****. The masking operation occurs within the LivePerson data centers when the session is concluded.

Access Control and Management

The LP Mobile environment (Amazon AWS) is maintained and operated by a dedicated team at LivePerson. Access to the LP Mobile environment (including EC2) is restricted to specific LivePerson personnel only (no Amazon personnel are granted access) on a need-to-work basis, and according to the least privilege security principle. Users that are granted this access require a unique SSH key to establish a connection, and can only do so over the minimal network ports that were approved. In addition, access to the AWS environment is based on a single sign-on and multi-factor authentication framework. The deployment of code can only be established when using a unique SSH key.

Security of System Components Hosted on Amazon

Operating Systems and Patch Management

LP Mobile servers are based on a hardened, minimal installation of Ubuntu Linux. The operating system is patched and updated on a regular basis. Each new version of LP Mobile includes an upgrade procedure for the OS and for the Application. Such upgrades and installations take place during maintenance windows, and on at least a quarterly basis.

Monitoring

The LP Mobile environment is constantly monitored by NOC and System Engineers. The monitoring tools include but are not limited to: Nagios, Zabbix, Graphite, Grafana, ELK (ElasticSearch/LogStash/Kibana). The parameters in scope of monitoring are both operational and security-related: Logs, CPU, performance, memory, collection of hardware information, and utilization.

Segregation of Duties and Software Deployment Process

Access to the S3 instance is based on security keys controlled by LivePerson, and is restricted to the appropriate authorized personnel on a need to work basis, and subject to change management processes. The deployment process copies the new files to the S3 bucket, and then proceeds to invalidate the cache. It is not possible for changes that did not originate from the S3 bucket to propagate to Cloudfront. All customer-specific files and chat/visit data is transferred only through LivePerson systems, not through S3 or Cloudfront.

Infrastructure and System Maintenance

Amazon is an Infrastructure as a Service (IaaS) provider that owns the physical equipment and is responsible for its housing, running and maintenance. Amazon (or any other 3rd party) is not authorized to access LivePerson components. LivePerson is fully responsible for managing and supporting the LP Mobile infrastructure. This includes: Firewall and network security configuration, operating system installation, administration and maintenance, storage management, CDN administration, patch management, uptime monitoring, and more. The responsibility for security is shared between Amazon and LivePerson: Amazon manages the underlying infrastructure, and LivePerson is responsible for securing and maintaining anything installed on top of that infrastructure. As stated earlier, all network communications between mobile devices and EC2, and between EC2 and LivePerson, is established over HTTPS utilizing TLS encryption.

Amazon Security

The AWS cloud infrastructure is designed to be one of the most flexible and secure cloud computing environments available today. It provides a highly reliable platform that enables customers to deploy applications and data quickly and securely. Prior to selecting AWS, LivePerson performed a risk assessment and due diligence process, and determined that the security controls and certifications provided by AWS exceed the industry standard. For more information (provided by AWS), please see below:

- http://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf
- https://cloudsecurityalliance.org/star-registrant/amazon-aws/

This document, materials or presentation, whether offered online or presented in hard copy ("LivePerson Informational Tools") is for informational purposes only. LIVEPERSON, INC. PROVIDES THESE LIVEPERSON INFORMATIONAL TOOLS "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

The LivePerson Informational Tools contain LivePerson proprietary and confidential materials. No part of the LivePerson Informational Tools may be modified, altered, reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the prior written permission of LivePerson, Inc., except as otherwise permitted by law. Prior to publication, reasonable effort was made to validate this information. The LivePerson Information Tools may include technical inaccuracies or typographical errors. Actual savings or results achieved may be different from those outlined in the LivePerson Informational Tools. The recipient shall not alter or remove any part of this statement.

Trademarks or service marks of LivePerson may not be used in any manner without LivePerson's express written consent. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies. LivePerson shall not be liable for any direct, indirect, incidental, special, consequential or exemplary damages, including but not limited to, damages for loss of profits, goodwill, use, data or other intangible losses resulting from the use or the inability to use the LivePerson Information Tools, including any information contained herein.

LIVEPERSON