Dooblo SurveyToGo: Security Overview

May, 2012

Written by:
Dooblo

Table of Contents

1 Introduction

1.1 Overview

This document outlines the security of the SurveyToGo system. All non-confidential information has been included. Due to the nature of the topics discussed, some topics are considered confidential and will not be discussed in this document for obvious reasons.

1.2 Purpose

The purpose of this document is to provide for a high level overview of all the security aspects of the SurveyToGo system. As the SurveyToGo system grows more security measures are added and infrastructure and communications protocols change. This document provides the overview for the system at the time of writing only.

2 Physical Data Center Security

2.1 Overview

The SurveyToGo state-of-the-art data center servers are hosted by Amazon AWS: AWS datacenters are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access datacenter floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. AWS only provides datacenter access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to datacenters by AWS employees is logged and audited routinely. For more extensive information about the AWS infrastructure security utilized by Dooblo: http://d36cz9buwru1tt.cloudfront.net/pdf/AWS_Security_Whitepaper.pdf

2.2 Servers

All servers include a mandatory antivirus protection and are configured to receive any security OS update as required.

2.3 Employee lifecycle

Dooblo has established formal policies and procedures to delineate the minimum standards for logical access to the SurveyToGo servers. Dooblo requires that staff with potential access to customer data undergo an extensive background check (as permitted by law) relevant to their position and level of data access.

3 Network Security

3.1 Overview

SurveyToGo enables interviewers in the field to collect data and send it over the wire to the Dooblo Data center. This involves 2 way communications over the internet to both send Survey data to the device and receive collected data from the device. The Dooblo network security measures are in place to ensure network communication both to and from the data center is secure along with communications between servers in the data center.

3.2 Connections from the devices to the data centers and back

The devices and management applications communicate over the internet with the Data center. SurveyToGo can utilize industry proven SSL encryption to encrypt these device/server communications and management app/server communications. The Dooblo Data Center uses certified SSL Certificates to ensure devices can validate and authenticate the server they are communicating with to prevent man in the middle attacks along with eavesdropping risks. Any incoming communication to the data center passes through a dedicated Checkpoint firewall product to prevent network attacks.

3.3 Connections between servers inside the data center

All servers in the data center are located in the same physical space and are connected through a dedicated sub-network controlled by authorized Dooblo IT employees. The Checkpoint Firewall ensures internal communication between DMZ and other servers is done only by pre-configured IP addresses.

3.4 Administrative communications

All administrative communications to the data center are secured with token based security and restricted to authorized personnel and IP addresses.

3.5 IDS/IPS

All network traffic stopped at the FW is monitored and IDS/IPS (Intrusion Detection/Prevention systems) is employed.

4 SurveyToGo Application Security Features

4.1 Overview

The SurveyToGo system includes application level security measures designed to allow your employees access to data only to those employees that you have configured and only to the project data that you have configured access for. SurveyToGo includes a customer-project paradigm which means that every data collected resides in a specific project that belongs to a specific customer (your customer, not Dooblo customers).

4.2 Users, types, groups & passwords

Each access to the SurveyToGo system is done with a user and a password. Surveyors have user names, so do project managers and field managers. Both data collection apps and the management studio app requires a user name and a password in order to work. In fact, every interface of the system requires an authenticated user in order to work. User names and passwords are defined by the SurveyToGo account administrator (NOT by Dooblo) and passwords are encrypted. Users can be grouped in to groups to help with permissions.

4.3 Role based permissions

Role based permissions are granted to users and projects. Each project has 4 levels of roles:

- Project Administrator
- Project Manager
- Project Reviewer
- Project Reader

Each role includes various access rights to the data contained in the project. The SurveyToGo account administrator (or project administrator/manager) can assign users or groups of users with the relevant roles of a project.
If a user does not have any access to a project that project will not show up on his management studio app. If the user does not have any access to any project of a customer than that entire customer will not show on his management app. Surveyor users can be assigned to a project which will then control whether they will see that survey in the list of surveys or not.

4.4 User rights

On top of the project “Role based” security, several application level user rights can be assigned to a user or a group such as:

- Create users
- Manage subject stores
- Manage rights
- Etc..

These rights are granted to the user or group and are not related to a specific customer or project.

5 SurveyToGo Data Collection App Security

5.1 Overview

The data collection apps are used to collect data from the field. The general approach to the security of the collected data in this regard is to upload the data and remove it from the device as quickly as possible. Shorter time on the device mean lower data security risks.

5.2 Android App

The Android app stores all data in a special application storage segment provided by the Android OS. This segment is secured from access by other applications and restricts the segment to the SurveyToGo app only. Due to this enhanced security mechanism by Android, the data is saved in a local database on this secured storage segment. When-ever network is detected, all data is uploaded to the server and deleted from the device. The last user who used the app is cached locally in order to allow for quick access and continue to collect data even in offline scenarios, however the password is encrypted. Communication to and from the server is secured by SSL Encryption (Optional) as described in the network security chapter.

5.3 PC Survey App

The PC (Windows) app stores all data in the local user storage space on the hard drive of the windows machine. As the hard disk is not secured like in the Android case, SurveyToGo utilizes the built-in encryption mechanism of Microsoft SQL Mobile to encrypt all the data and prevent access to it from unauthorized sources. Communication to and from the server is secured by SSL Encryption (Optional) as described in the network security chapter.

5.4 Lost / stolen Device

In case the device is lost or stolen it is our recommendation that the user of that device will be set to disabled. This will disallow any access from that device to the account and prevent any tampering with data. Please note that if auto-sync is enabled up to 10 minutes worth of data collection might remain on the device and be exposed.

6 Configuration Management

6.1 Overview

Configuration changes to the SurveyToGo system infrastructure and software are authorized, logged, tested, approved, and documented in accordance with industry norms. Updates to the SurveyToGo infrastructure are done to minimize any impact on the customer and their use of the services. Dooblo communicates with customers via email when service use is likely to be impacted.

6.2 Software

Dooblo applies a systematic approach to managing change so that changes to customer impacting services are thoroughly reviewed, tested, approved and well communicated.

Dooblos change management process is designed avoid unintended service disruptions and to maintain the integrity of service to the customer. Changes deployed into production environments are:

- Reviewed: Peer reviews of the technical aspects of a change
- Tested: being applied will behave as expected and not adversely impact performance
- Approved: to provide appropriate oversight and understanding of business impact

Changes are typically pushed into production in a phased deployment starting with customers who requested the change. When possible, changes are scheduled during weekend change windows. Emergency changes might be deployed on non standard times.

6.3 Infrastructure

Updates to the SurveyToGo infrastructure are done to minimize any impact on the customer and their use of the services. Dooblo communicates with customers via email when service use is likely to be impacted.

7 Backups

7.1 Overview

Data stored in the SurveyToGo system, is redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge. In addition, Dooblo periodically backs up all important parts of its data. Data removed from the system by actions of the customer are physically deleted from the servers and backups and will not be available to Dooblo support staff or customer. This is to ensure customer ability to *remove* sensitive information from the Dooblo Data center if needed.