DRAFT

MOBILE APP LOGIN ISSUE DETECTION

Capstone Project: Milestone Report

Springboard Foundations of Data Science

Donald Gennetten

Client & Business Value

With increasing speed to market pressures, technology teams are continually balancing their resource investment in technical debit against feature development. This can result in problems detecting issues (or impact) which then lead to unresolved problems, reduced market share and customer dissatisfaction.

The goal of this project is to identity Mobile App login issues that may not be clearly evident to the business and establish statistically confident correlations with problematic devices, operating system versions, authentication methods and application versions.

- **Business/Product Owners** will have improved visibility of issues allowing them to refine adoption projections and drive prioritization of enhancements and fixes.

- **Platform/Technology/DevOps** teams will be able to identity production support, capacity and infrastructure needs.

DRAFT

Dataset

Data is extracted from APIs, activity logs, and publicly available device manufacturer lists.

Limitations

- Sensitive or proprietary data is excluded from the data and therefore not available for analysis. This is assumed to have a low likelihood of impacting the final output.
- Login attempts resulting in a critical device level failures, and/or without a connection to the API, will not be reflected in the data. These failures will therefore not be reflected in this analysis.
- Login volumes will be aggregated at the hour. Any benefit from having unique records for each individual attempt will be lost. This is also assumed to have a low likelihood of impacting the final output.

Cleaning & Wrangling

API and activity log data is collected and aggregated from Splunk and internal data warehouse sources. Wrangling, analysis, summarization and visualization is conducted in R.

DRAFT

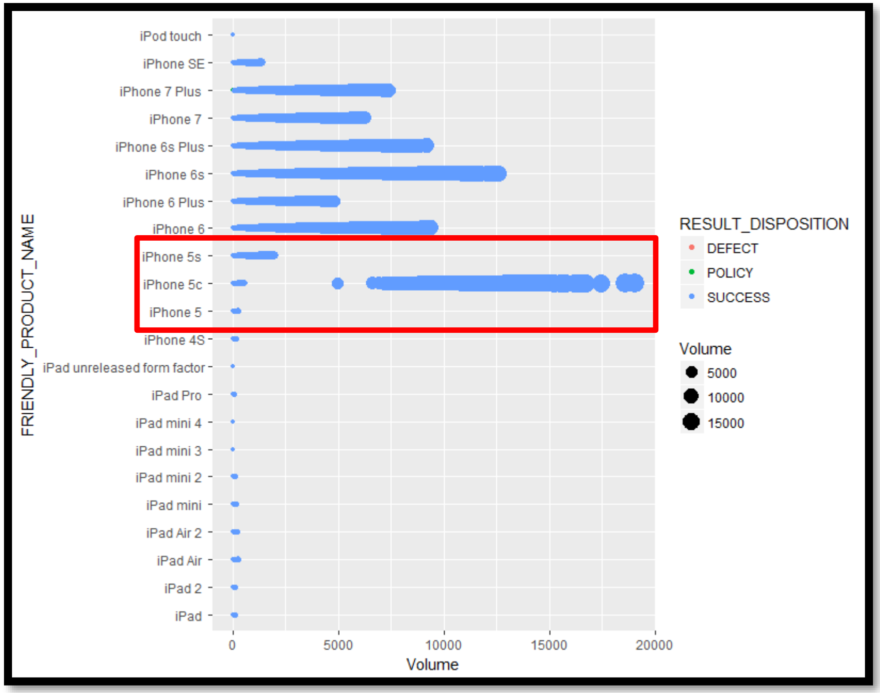
Dataset – Important Fields

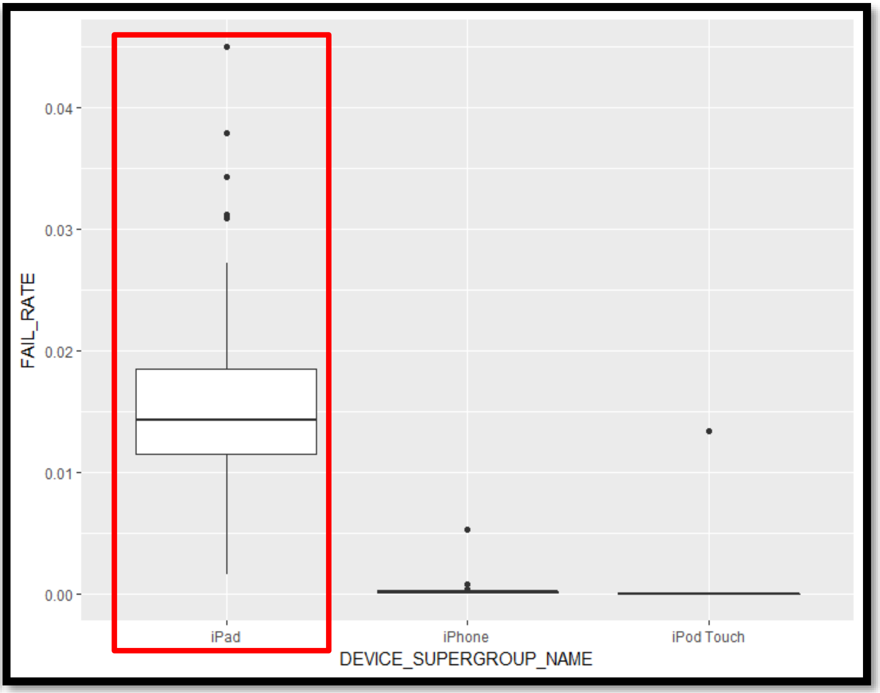
Source	Field Name	Sample Values	Definition
Internal API & Activity Logs	APP_VERSION	5.16.0, 5.15.0, 1613150500,	Code version for the installed mobile application
	AUTH_METHOD	Password, Finger Print, Pattern	Login method used by the user to authenticate
	CHANNEL__TYPE	MOBILE, WEB	Channel used by the customer during Login. Always expected to be “MOBILE”.
	DEVICE_OPERATING_SYSTEM	iOS, Android, iPhone OS	Operating system installed on the mobile device
	DEVICE_OPERATING_SYSTEM_VERSION	10.2.1, 6.0.1, 9.3	Operating system version installed on the mobile device
	APP_TYPE	iPhone, Android, iPad	App type installed on the device
	RESULT_DISPOSITION	SUCCESS, POLICY, DEFECT	General business result from a login attempt. SUCCESS = Successful login, DEFECT = Failed login due to technical issue, POLICY = Failed login due to business rule (Ex: Invalid ID/PWD)
Both	DEVICE_MODEL	iPhone5,3, iPhone8,1	Unique device model identifier. Used as lookup to get friendly product names
Manufacturer Device Information	FRIENDLY_PRODUCT_NAME	iPhone 6, iPhone 6s Plus, iPad mini	Commonly recognized marketing device names established by the Manufacturer

DRAFT

Preliminary Findings*

There is a significant population of iPhone 5C users	There are elevated failure rates within the iPad populations





* The above charts are illustrative of preliminary findings

Approach

1. Collect aggregate hourly login volumes for at least 1 month of login activity, with identified important fields.
2. Collect device model ID to common device name data for lookup and join purposes (ex: iPhone9,1 to iPhone 7).
3. Import, wrangle, clean & join datasets.
4. Explore high level volume, policy and failure rates.
5. Investigate volume patterns, disproportionate failure and policy rates, and any other notable observations.
6. Publish summary of results on GitHub to include README, slide deck report, sample data, and R code.