PolicyLock

Contributors: **Alex Oaten, Dean Sadaoka, Nick Allen, Sebastien Callait**

Supervisors: **Professor Davide Falessi & Industry Expert Matteo**

CALIFORNIA POLYTECHNIC STATE UNIVERSITY

TABLE OF CONTENTS

INTRODUCTION

Aim of the Document

This document will describe the PolicyLock software, it's functionalities, use cases, design decisions, and how it will look and operate, in order to create a holistic and accurate understanding of the software and it's intended uses.

Overview of the Defined System

PolicyLock enables system supervisors to monitor the devices on their network for potential trojan horse-like malware. This is done through an interface in which a supervisor can view and control application permissions for all devices on their network, become notified of suspicious application behaviour, view logs of all incoming and past permission requests, and monitor application feature usage.

Operational Settings

PolicyLock can be restricted to only monitor certain devices and applications as a means to reduce the requirements for it to be run. At a minimum, however, it should be run on a device with at least 2GB RAM, a processor 1GHZ or higher, and at least 500MB of free memory.

Competitors

Competitors mostly exist in the form of permission management applications, therefore it makes sense to list some of the most common ones and how they compare to PolicyLock:

1. Android Permission Manager

Pros	Cons
App provides many protection features and application usage details	Only works on Android Devices
High rating on Android store (4.1 / 5)	Bugs reported on certain devices
Free plan available	Ads on free plan take away from user experience

2. MyPermissions

Pros	Cons
Interface is intuitive and easy to learn.	Only works on Android Devices
Free plan available	Many bugs reported with recent updates
	Free version doesn't allow for revoking application permissions

In comparison with these competitors, PolicyLock offers similar functionality but for desktop. The other major distinction is that PolicyLock grants the ability for a supervisor to monitor the applications of all devices on a network, as opposed to just a single device.

USER STORIES

1. As a supervisor, I want to log in, so that only authenticated users can access the application.

2. As a supervisor, I want to view all of a device's applications, so that I can see if there are any apps that the device should not have.

3. As a supervisor, I want to view all of the devices the application monitors, so that I can easily see all devices I supervise.

4. As a supervisor, I want to view, add, or revoke permissions for an application, so that I can change the permissions for an application if needed.

5. As a supervisor, I want to have an option to revoke all permissions, so that I can quickly disable a rogue device or application.

6. As a supervisor, I want to compare an app's permission settings to the app's manifest, so that I can see if there are any permissions that the app has access to that it should not need.

7. As a supervisor, I want to have the option to log an application's usage of a permitted feature, so that I am aware of the usage of certain features.

8. As a supervisor, I want to have four warning levels (info, notice, warning, and critical), so that I am able to quickly differentiate the importance of the notification.

9. As a supervisor, I want to be notified for notice, warning, and critical warning levels, so that I am able to immediately respond to an attempted unauthorized feature usage.

10. As a supervisor, I want to have the option to only be notified for warning and critical warning levels, so that I am not overwhelmed with notifications.

11. As a supervisor, I want to be sent a notification either as a push, email, or both, so that I am able to view the notifications in the most convenient way for me.

12. As a supervisor, I want to view a log of an application’s feature usage, so that I can monitor applications for unusual feature usage.

13. As a supervisor, I want to save logs as an excel file, so that I am able to easily move and view logs outside of the system.

14. As a supervisor, I want to change the logging settings, so that I can adjust the logging level to the amount of storage I have available.

15. As a supervisor, I want to be notified when an application the system isn't aware of attempts to run, so that I can immediately address the threat.

16. As a supervisor, I want to use permitted features without interruption, so that the application is able to work normally.

FUNCTIONAL REQUIREMENTS

1. The system shall provide a list of permissions an application requests in the app manifest*.

2. The system shall provide a warning label to every message of either info, notice, warning or critical.

3. The system shall provide email and push notifications for notice, warning, and critical level messages.

4. The system shall provide a notification setting to notify via email, push, or both.

5. The system shall provide a notification setting to only notify for warning and critical level messages.

6. The system shall provide a notification when an application attempts to use an unauthorized feature.

7. The system shall provide a notification when an unknown application attempts to run on a device.

8. The system shall provide logging of all activities of a device.

9. The system shall provide log save settings of verbose*, standard*, or minimal* logging.

10. The system shall provide a comparison of applications' permitted features* and features* it attempts to access.

11. The system shall provide permission settings.

12. The system shall provide a permission setting to revoke all permissions for an application.

13. The system shall provide a permission setting to revoke all permissions for a user.

14. The system shall provide an application access to authorized features.

15. The system shall provide background monitoring of applications' feature* usage.

DICTIONARY

---

app manifest - Describes essential information about the app which includes the permissions that the app needs in order to access protected parts of the system or other apps.

feature - Protected parts of a computer system like browsing, location data, photos, etc.

Warning levels:

1. **INFO -** Informational messages that require no action. This includes all pertinent information (device logins, logouts, permission requests, feature usage, etc.).
2. **NOTICE -** Normal, but significant events. This is when an application or user uses a feature that was set to be monitored in the settings.
3. **WARNING -** Warning conditions that should be taken care of. This is when an application attempts to use a non-permitted feature.
4. **CRITICAL -** Critical conditions. This is when an application runs that the system was not aware of or when a known application attempts to use multiple non-permitted features, or when a known application attempts to use a non-permitted feature multiple times.

Logging Levels:

1. **VERBOSE -** Includes INFO, NOTICE, WARNING, CRITICAL.
2. **STANDARD -** Includes NOTICE, WARNING, CRITICAL.
3. **MINIMAL -** Includes WARNING, CRITICAL.

USE CASES (INTERNAL STEPS)

Name: Change an application's permissions

1. The supervisor logs in.
2. The system displays a list of devices.
3. The supervisor selects a specific device.
4. The system displays a list of the device's applications.
5. The supervisor selects the application to change its permissions.
6. The system displays a list of the application's permissions.
7. The supervisor selects the permission(s) they would like to change.
8. The supervisor saves the changes and exits.
9. The system logs, implements the changes, and exits.

Extensions:

7a. *The supervisor does not make any changes*: The system does not log or save anything.
7b. *The supervisor exits without saving the changes*: The system prompts the user if they want to "Cancel" or "Save Changes".
8a. *The system fails to implement the changes*: The system notifies the supervisor that it wasn't able to implement the change.

Name: Change log settings

1. The supervisor logs in.
2. The supervisor opens "Log".
3. The supervisor opens "Logging Settings".
4. The system displays current logging settings.
5. The supervisor selects preferred logging setting.
6. The supervisor clicks "Save" button.
7. The system saves the settings and exits back to home.

Extensions:

2a. *Database is full:* The system warns the supervisor that the database is full.
5a. *Supervisor has not selected a logging setting*: System prompts supervisor to select a logging setting before they can save and exit.
5b. *Supervisor has selected multiple logging settings*: System prompts supervisor to select only one logging setting before they can save and exit.

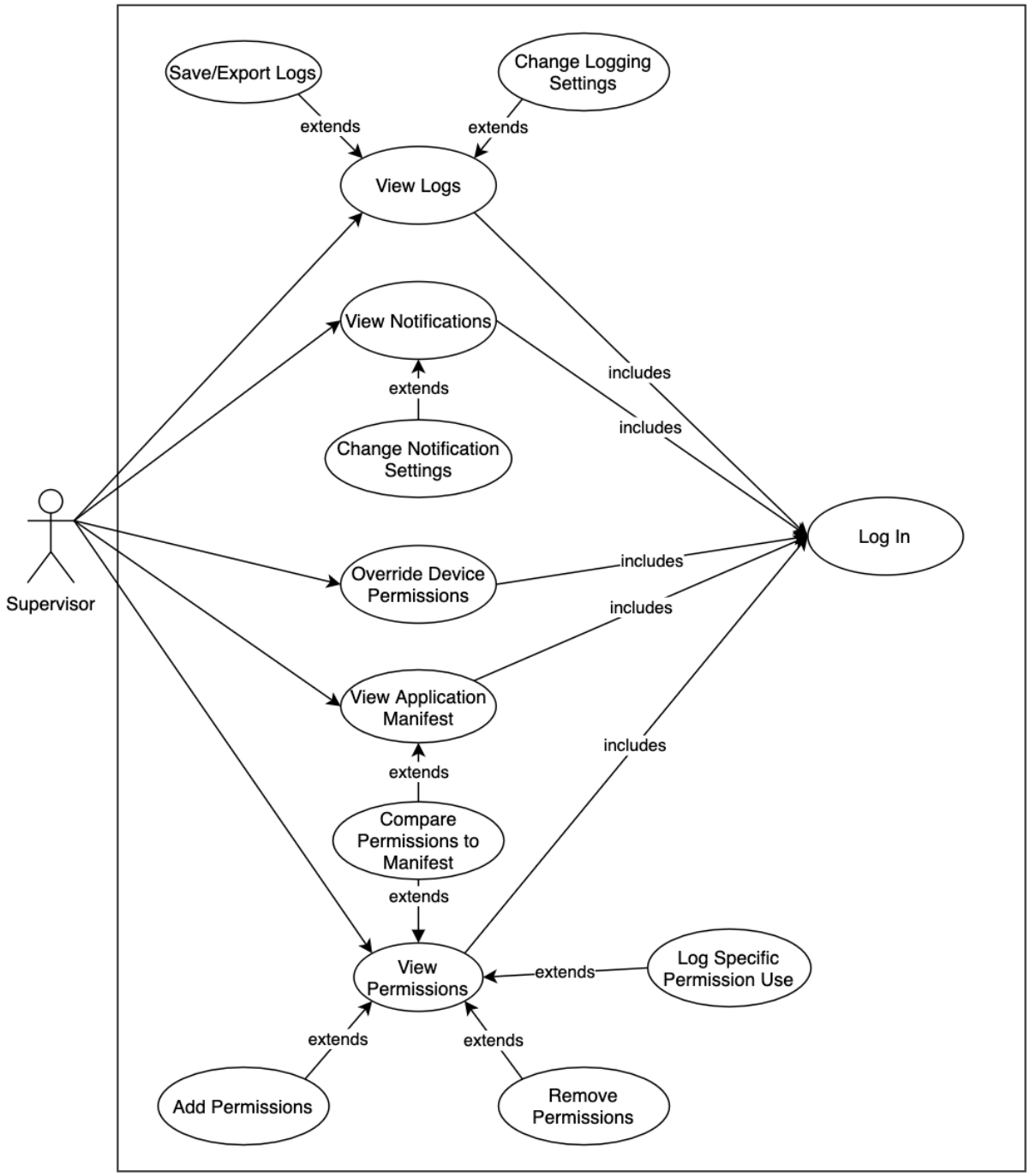
Name: Compare given application permissions with manifest
1. The supervisor logs in.
2. The system displays a list of devices.
3. The supervisor selects a specific device.
4. The system displays a list of the device's applications.
5. The supervisor selects the specific application.
6. The supervisor presses the manifest button.
7. The system shows the application's manifest.
8. The supervisor presses the compare permissions button.
9. The system gives an "everything looks good" alert.

Extensions:
2a. *There are no devices set up in the system:* The system displays a message that there are no devices added to the system.
8a. *Permissions are used that aren't in manifest*: The system displays and logs a warning with a list of the permissions that aren't in the manifest.
8b. *Permissions not given that are requested in the manifest:* The system displays the permissions requested in the manifest that aren't given to the application.

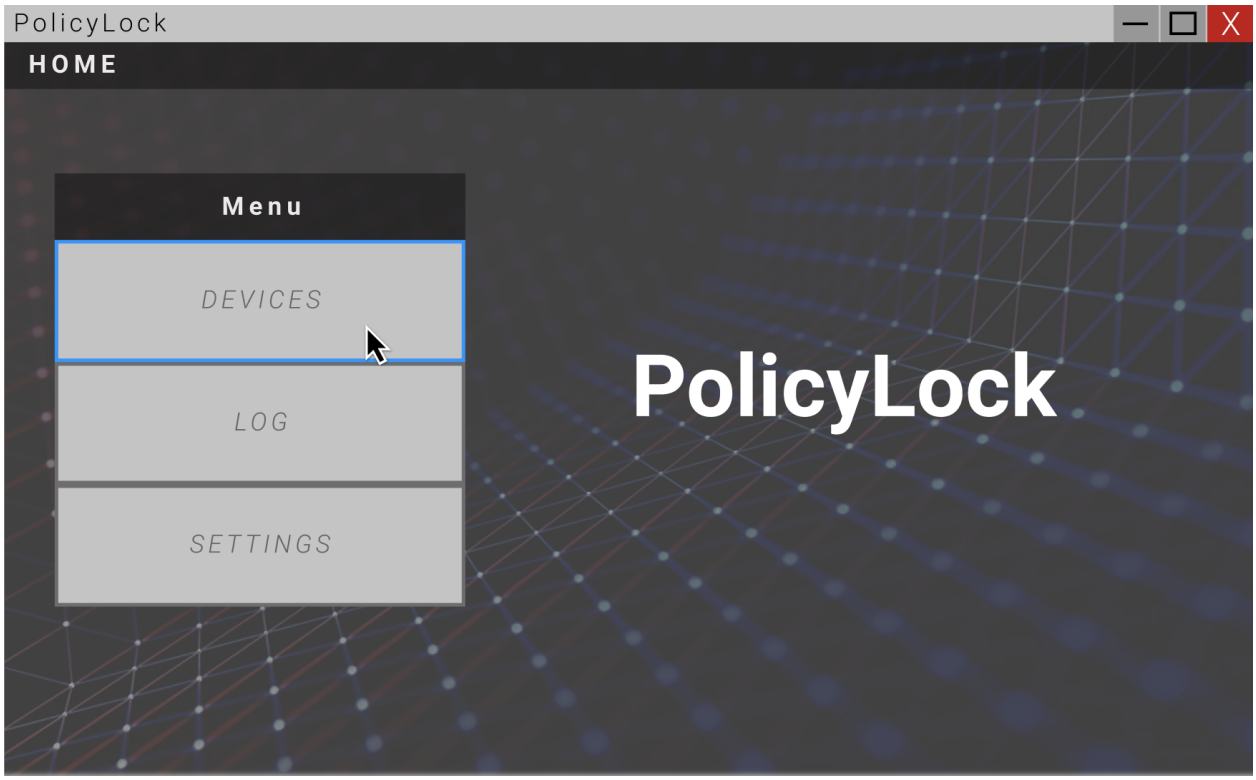
Name: Override device permissions
1. The supervisor logs in.
2. The system displays a list of devices.
3. The supervisor selects a specific device.
4. The supervisor selects "Device Settings".
5. The supervisor selects the "Override Device Permissions" option.
6. The system redacts permission to all features of the device.
7. The system alerts the supervisor with a confirmation message.

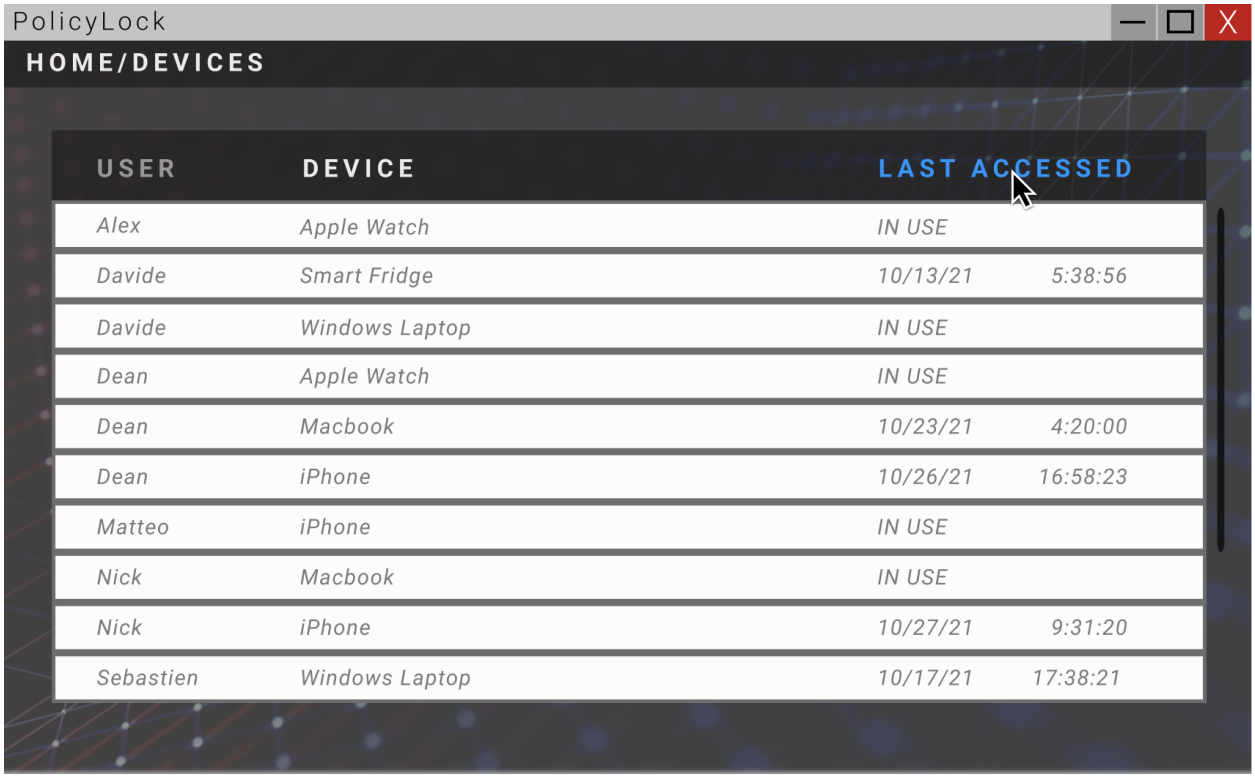
Extensions:
2a. *There are no devices in the system:* The system displays a message saying that there are no devices in the system.
7a. *System fails to redact all device permissions:* The system notifies the user that it failed to redact all permissions.
7b. *Application in use requires permission:* The system notifies the user that an application is currently using a device feature and prompts the user to confirm that they still want to redact permissions.

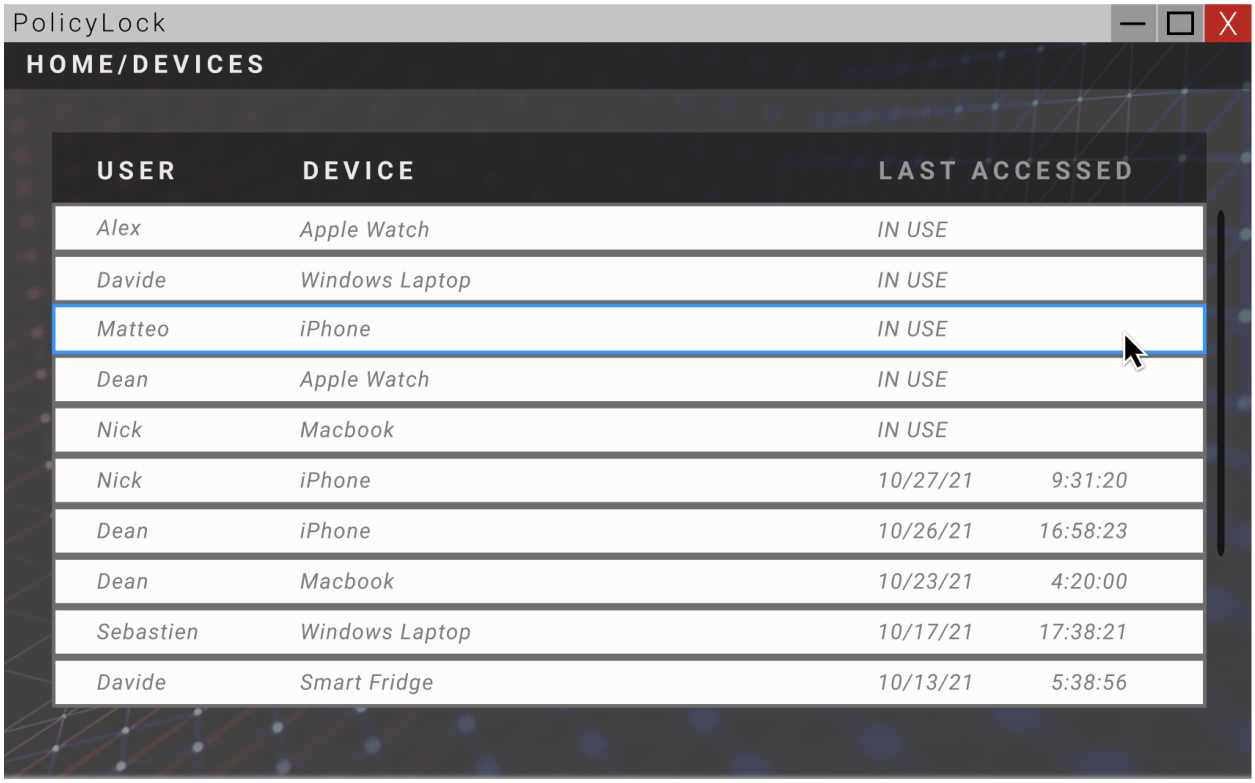
USE CASE DIAGRAM

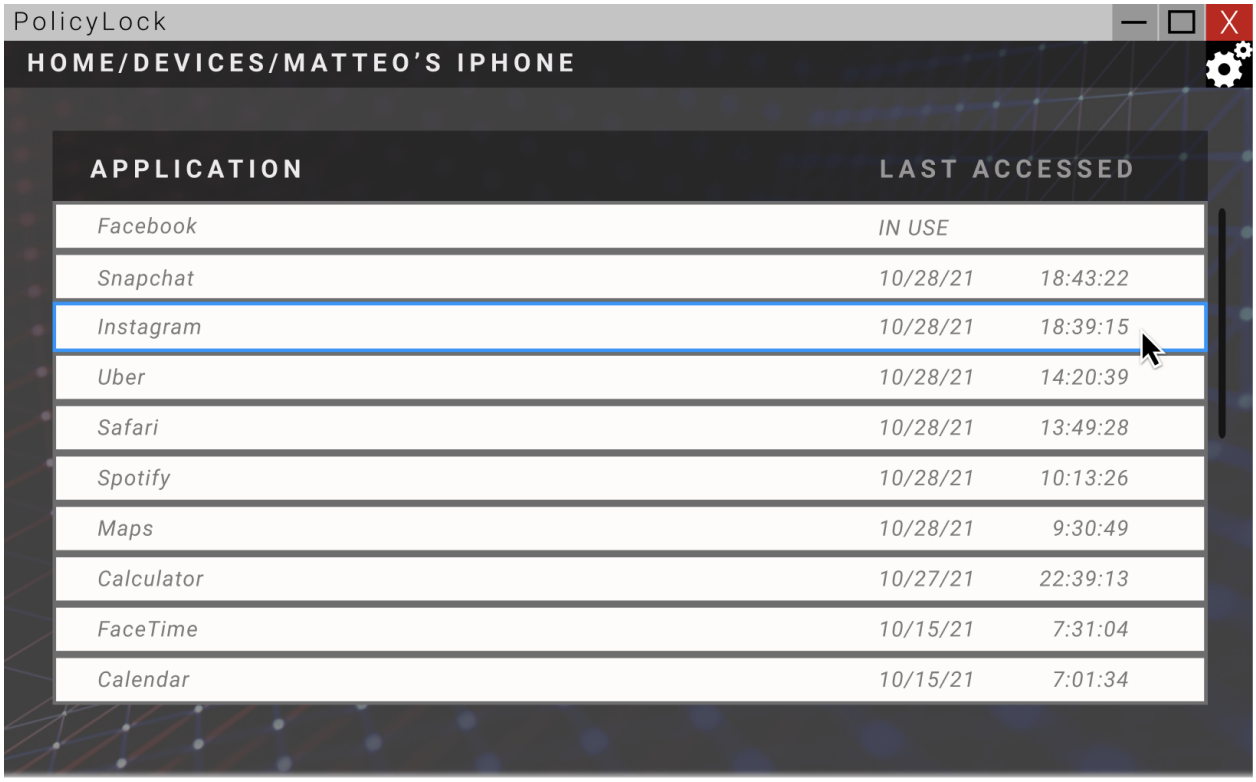


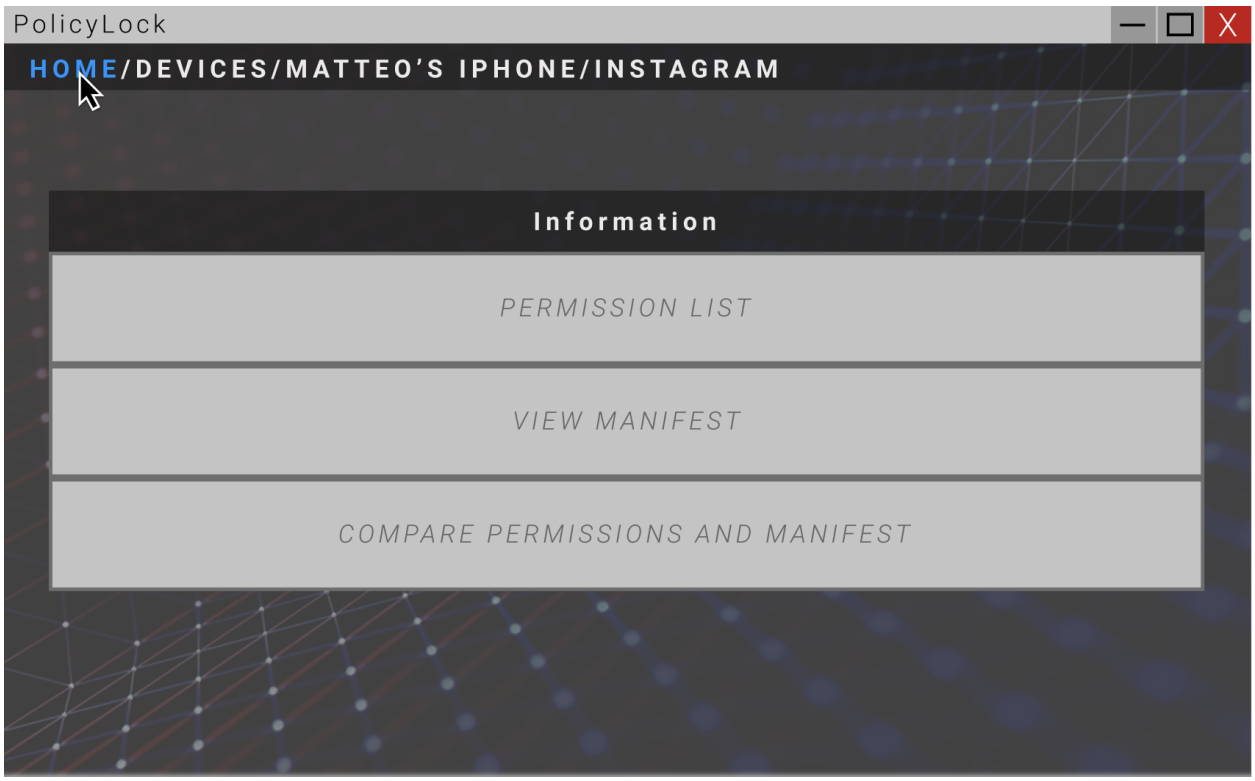
STORYBOARDS

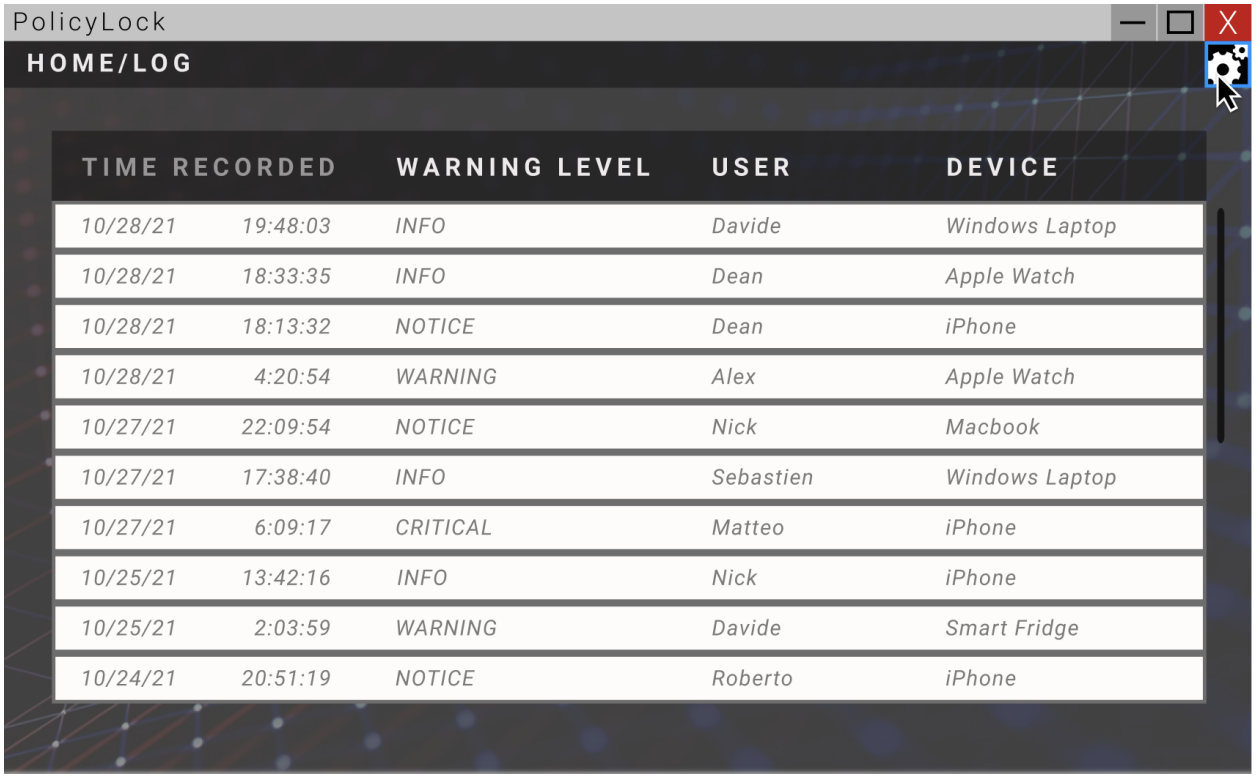


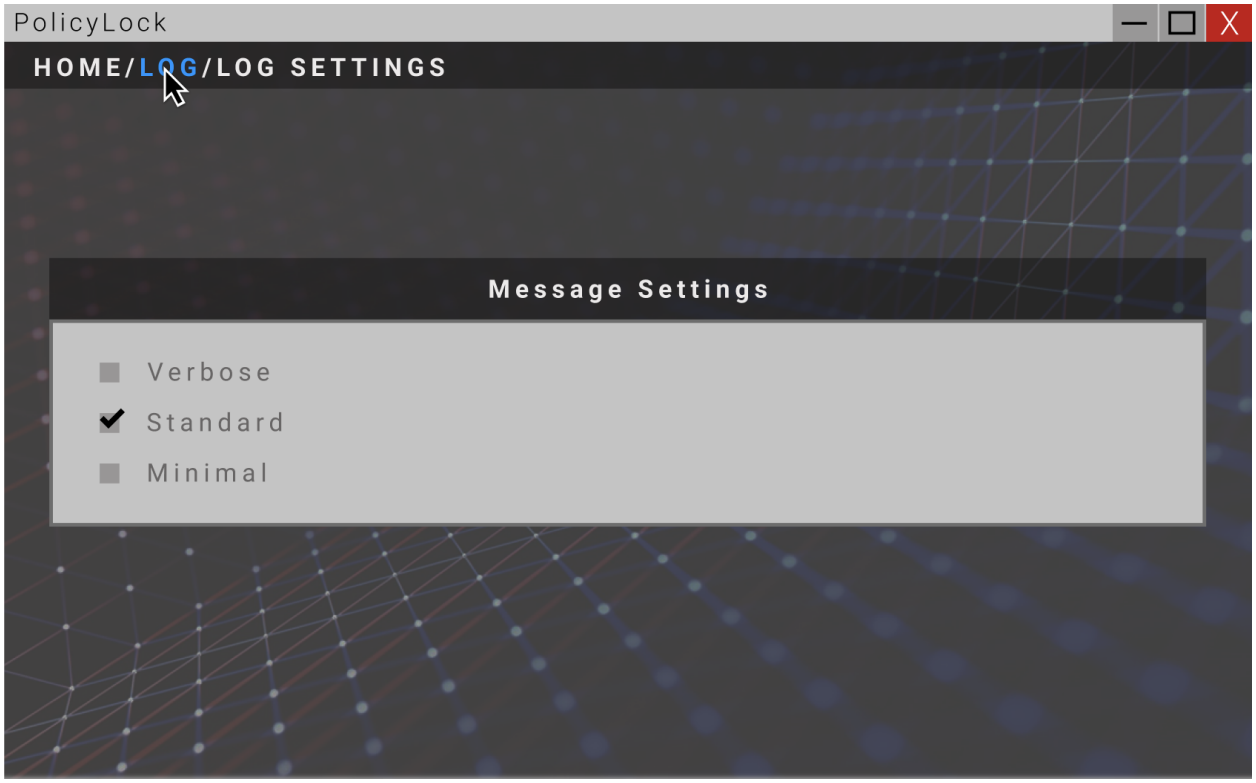

PolicyLock
HOME/DEVICES
USER
DEVICE
LAST ACCESSED
Alex Apple Watch IN USE
Davide Smart Fridge 10/13/21 5:38:56
Davide Windows Laptop IN USE
Dean Apple Watch IN USE
Dean Macbook 10/23/21 4:20:00
Dean iPhone 10/26/21 16:58:23
Matteo iPhone IN USE
Nick Macbook IN USE
Nick iPhone 10/27/21 9:31:20
Sebastien Windows Laptop 10/17/21 17:38:21

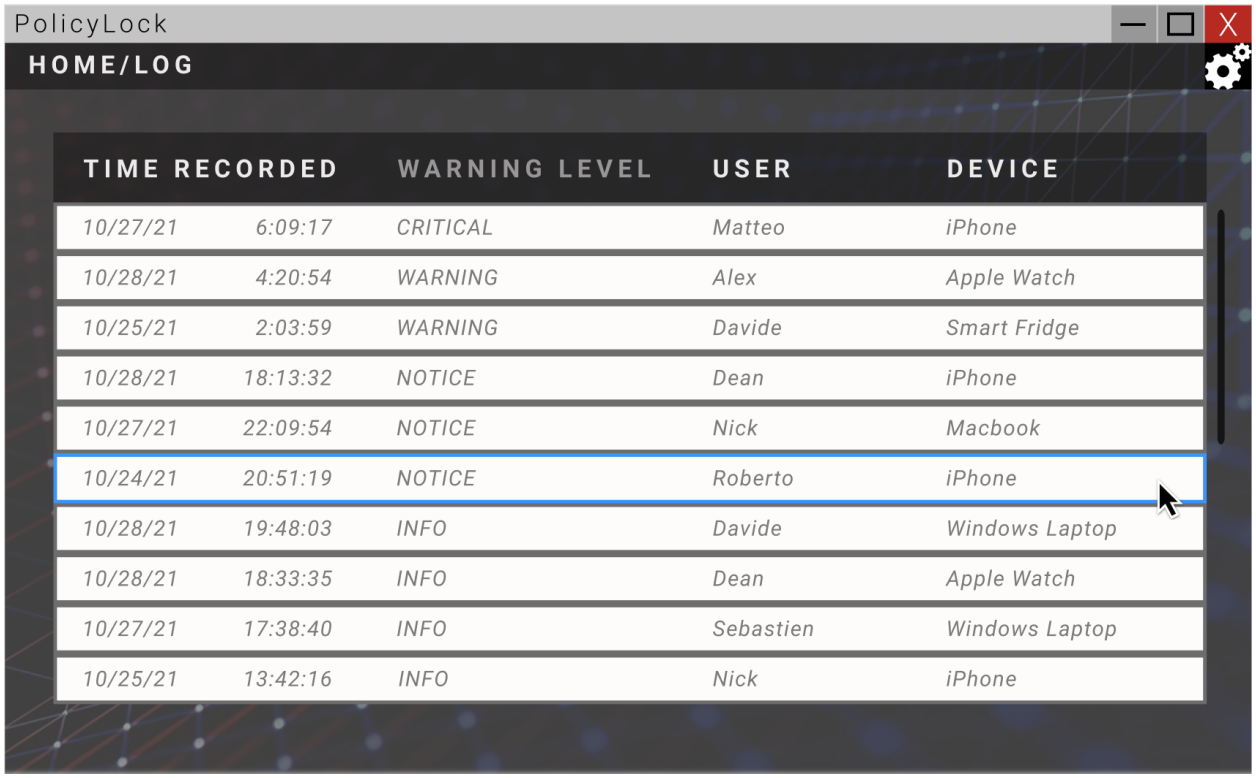

PolicyLock
HOME/DEVICES
USER
DEVICE
LAST ACCESSED
Alex Apple Watch IN USE
Davide Windows Laptop IN USE
Matteo iPhone IN USE
Dean Apple Watch IN USE
Nick Macbook IN USE
Nick iPhone 10/27/21 9:31:20
Dean iPhone 10/26/21 16:58:23
Dean Macbook 10/23/21 4:20:00
Sebastien Windows Laptop 10/17/21 17:38:21
Davide Smart Fridge 10/13/21 5:38:56

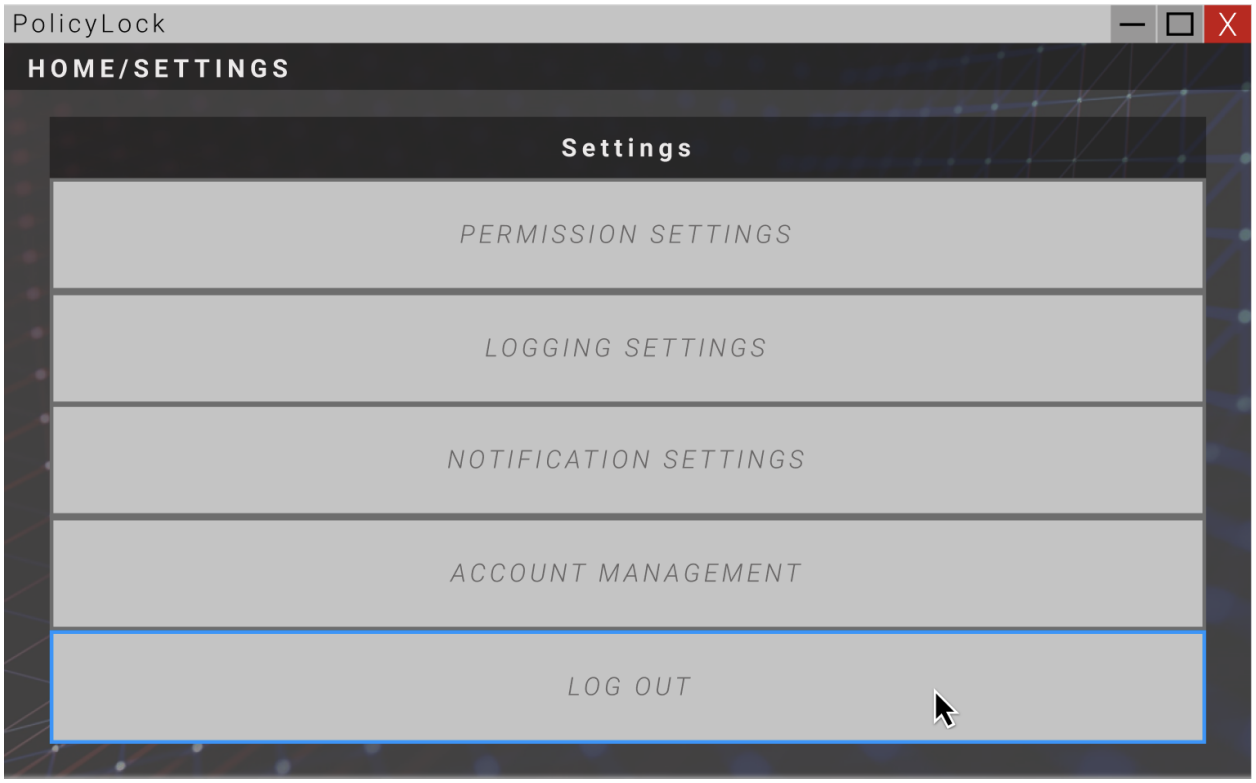

PolicyLock
HOME/DEVICES/MATTEO'S IPHONE
APPLICATION
LAST ACCESSED
Facebook
IN USE
Snapchat
10/28/21
18:43:22
Instagram
10/28/21
18:39:15
Uber
10/28/21
14:20:39
Safari
10/28/21
13:49:28
Spotify
10/28/21
10:13:26
Maps
10/28/21
9:30:49
Calculator
10/27/21
22:39:13
FaceTime
10/15/21
7:31:04
Calendar
10/15/21
7:01:34


PolicyLock
HOME/DEVICES/MATTEO'S IPHONE/INSTAGRAM
Information
PERMISSION LIST
VIEW MANIFEST
COMPARE PERMISSIONS AND MANIFEST


PolicyLock
HOME/LOG
TIME RECORDED
WARNING LEVEL
USER
DEVICE
10/28/21 19:48:03 INFO Davide Windows Laptop
10/28/21 18:33:35 INFO Dean Apple Watch
10/28/21 18:13:32 NOTICE Dean iPhone
10/28/21 4:20:54 WARNING Alex Apple Watch
10/27/21 22:09:54 NOTICE Nick Macbook
10/27/21 17:38:40 INFO Sebastien Windows Laptop
10/27/21 6:09:17 CRITICAL Matteo iPhone
10/25/21 13:42:16 INFO Nick iPhone
10/25/21 2:03:59 WARNING Davide Smart Fridge
10/24/21 20:51:19 NOTICE Roberto iPhone


PolicyLock
HOME/LOG/LOG SETTINGS
Message Settings
Verbose
Standard
Minimal


PolicyLock
HOME/LOG
TIME RECORDED
WARNING LEVEL
USER
DEVICE
10/27/21 6:09:17 CRITICAL Matteo iPhone
10/28/21 4:20:54 WARNING Alex Apple Watch
10/25/21 2:03:59 WARNING Davide Smart Fridge
10/28/21 18:13:32 NOTICE Dean iPhone
10/27/21 22:09:54 NOTICE Nick Macbook
10/24/21 20:51:19 NOTICE Roberto iPhone
10/28/21 19:48:03 INFO Davide Windows Laptop
10/28/21 18:33:35 INFO Dean Apple Watch
10/27/21 17:38:40 INFO Sebastien Windows Laptop
10/25/21 13:42:16 INFO Nick iPhone


PolicyLock
HOME/SETTINGS
Settings
PERMISSION SETTINGS
LOGGING SETTINGS
NOTIFICATION SETTINGS
ACCOUNT MANAGEMENT
LOG OUT

AHP

R1: The system shall provide logging of all activities of a device
R2: The system shall provide an option to revoke all permissions for an application
R3: The system shall provide a comparison of applications' permitted features and features it attempts to access
R4: The system shall provide background monitoring of applications' feature usage

Cost	R1	R2	R3	R4
R1	1	1/3	6	2
R2	3	1	7	4
R3	1/6	1/7	1	1/4
R4	1/2	1/4	4	1
Column Sum	4.67	1.73	18.00	7.25

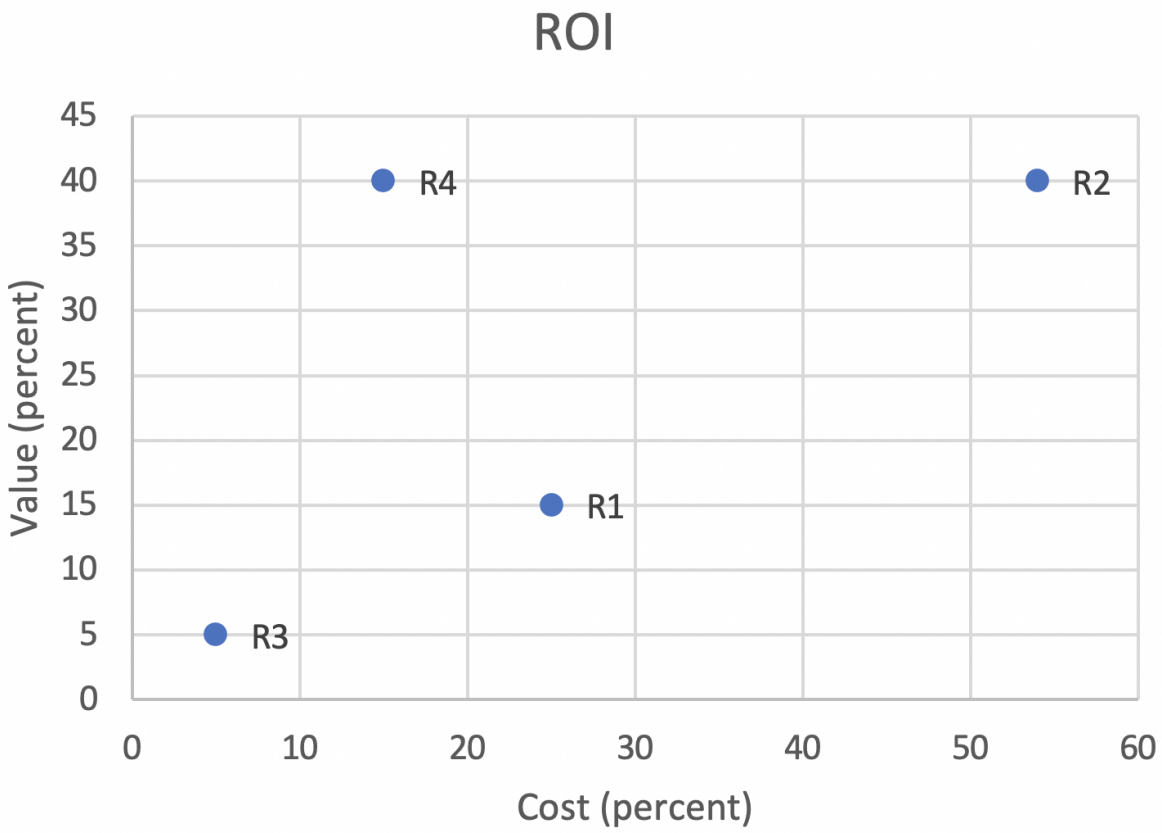
Value	R1	R2	R3	R4
R1	1	1/4	6	1/4
R2	4	1	7	1
R3	1/6	1/7	1	1/7
R4	4	1	7	1
Column Sum	9.17	2.39	21.00	2.39

Cost	R1	R2	R3	R4
R1	0.21	0.19	0.33	0.28
R2	0.64	0.58	0.39	0.55
R3	0.04	0.08	0.06	0.03
R4	0.11	0.14	0.22	0.14

Row Sum	Sum/4
1.02	0.25
2.16	0.54
0.21	0.05
0.61	0.15

Value	R1	R2	R3	R4
R1	0.11	0.10	0.29	0.10
R2	0.44	0.42	0.33	0.42
R3	0.02	0.06	0.05	0.06
R4	0.44	0.42	0.33	0.42

Row Sum	Sum/4
0.60	0.15
1.61	0.40
0.19	0.05
1.61	0.40



R1: The system shall provide logging of all activities of a device
R2: The system shall provide a notification when an unknown application attempts to run on a device
R3: The system shall provide permission settings
R4: The system shall provide a notification when an application attempts to use an unauthorized feature

Cost	R1	R2	R3	R4
R1	1	1/5	1/4	1/2
R2	5	1	1/2	2
R3	4	2	1	3
R4	2	1/2	1/3	1
Column Sum	12.00	3.70	2.08	6.50

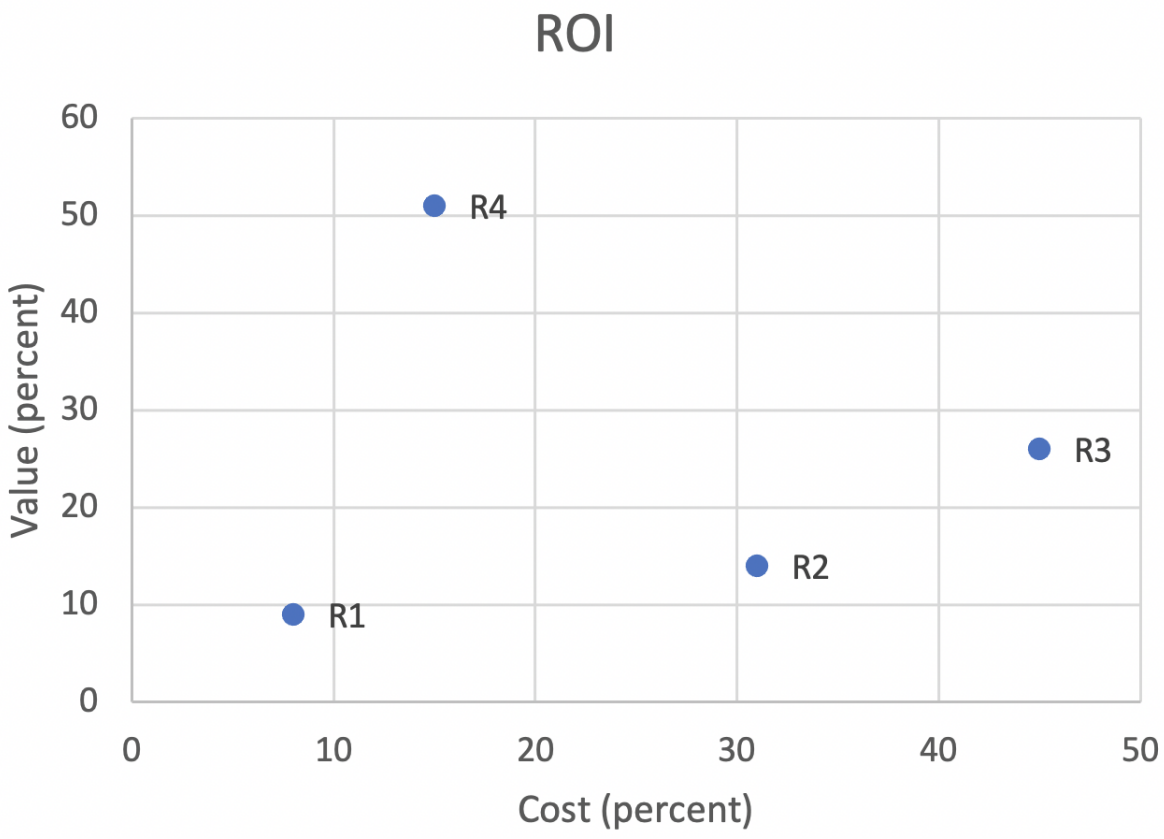
Value	R1	R2	R3	R4
R1	1	1/2	1/3	1/4
R2	2	1	1/2	1/5
R3	3	2	1	1/2
R4	4	5	2	1
Column Sum	10.00	8.50	3.83	1.95

Cost	R1	R2	R3	R4
R1	0.08	0.05	0.12	0.08
R2	0.42	0.27	0.24	0.31
R3	0.33	0.54	0.48	0.46
R4	0.17	0.14	0.16	0.15

Row Sum	Sum/4
0.33	0.08
1.23	0.31
1.82	0.45
0.62	0.15

Value	R1	R2	R3	R4
R1	0.10	0.06	0.09	0.13
R2	0.20	0.12	0.13	0.10
R3	0.30	0.24	0.26	0.26
R4	0.40	0.59	0.52	0.51

Row Sum	Sum/4
0.37	0.09
0.55	0.14
1.05	0.26
2.02	0.51



R1: The system shall provide a notification option to only notify for warning and critical level messages
R2: The system shall provide a permission setting to revoke all permissions for an application
R3: The system shall provide a permission setting to revoke all permissions for a user
R4: The system shall provide a list of permissions an application requests in the app manifest

Cost	R1	R2	R3	R4
R1	1	1/5	1/5	1
R2	5	1	1	5
R3	5	1	1	5
R4	1	1/5	1/5	1
Column Sum	12.00	2.40	2.40	12.00

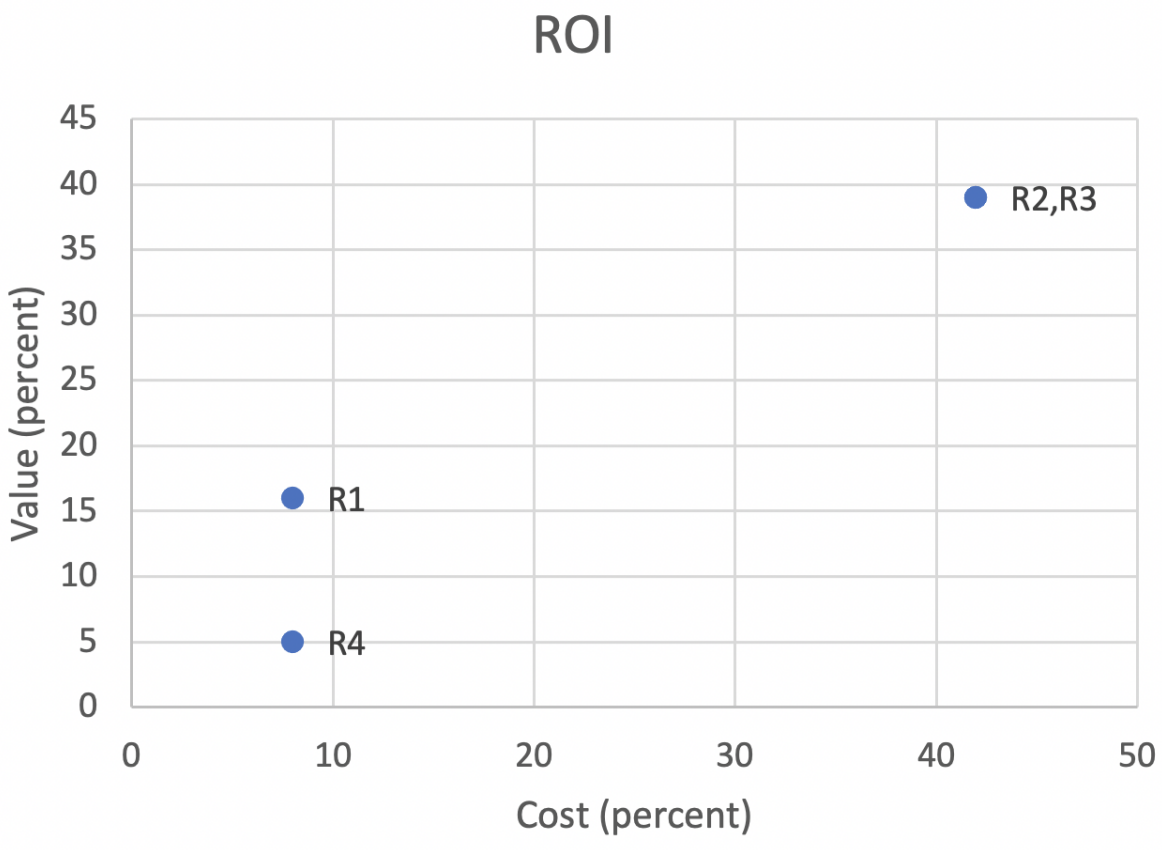
Value	R1	R2	R3	R4
R1	1	1/3	1/3	5
R2	3	1	1	7
R3	3	1	1	7
R4	1/5	1/7	1/7	1
Column Sum	7.20	2.48	2.48	20.00

Cost	R1	R2	R3	R4
R1	0.08	0.08	0.08	0.08
R2	0.42	0.42	0.42	0.42
R3	0.42	0.42	0.42	0.42
R4	0.08	0.08	0.08	0.08

Row Sum	Sum/4
0.33	0.08
1.67	0.42
1.67	0.42
0.33	0.08

Value	R1	R2	R3	R4
R1	0.14	0.13	0.13	0.25
R2	0.42	0.40	0.40	0.35
R3	0.42	0.40	0.40	0.35
R4	0.03	0.06	0.06	0.05

Row Sum	Sum/4
0.66	0.16
1.57	0.39
1.57	0.39
0.19	0.05



R1: The system shall provide an application access to authorized features
R2: The system shall provide permission settings
R3: The system shall provide logging of all activities of a device
R4: The system shall provide email and push notifications for notice, warning, and critical level messages

Cost	R1	R2	R3	R4
R1	1	1	3	7
R2	1	1	3	7
R3	1/3	1/3	1	5
R4	1/7	1/7	1/5	1
Column Sum	2.48	2.48	7.20	20.00

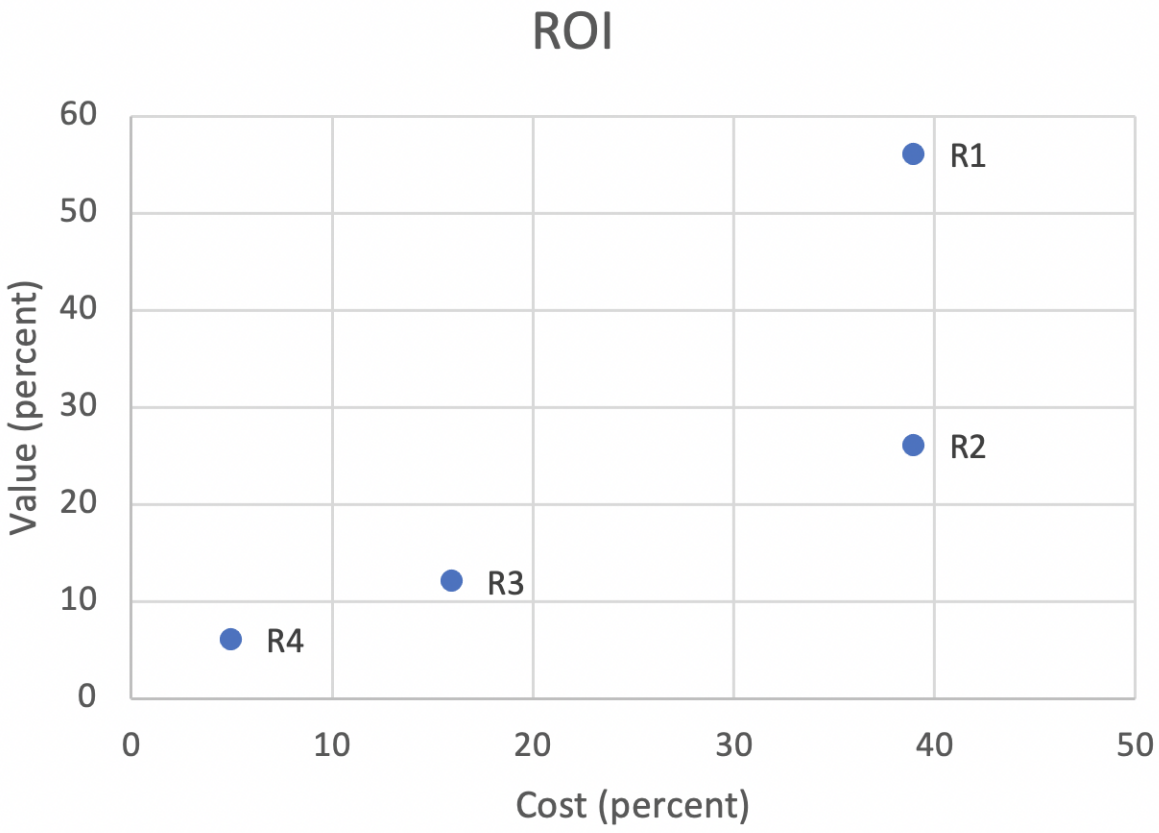
Value	R1	R2	R3	R4
R1	1	3	5	7
R2	1/3	1	3	5
R3	1/5	1/3	1	3
R4	1/7	1/5	1/3	1
Column Sum	1.68	4.53	9.33	16.00

Cost	R1	R2	R3	R4
R1	0.40	0.40	0.42	0.35
R2	0.40	0.40	0.42	0.35
R3	0.13	0.13	0.14	0.25
R4	0.06	0.06	0.03	0.05

Row Sum	Sum/4
1.57	0.39
1.57	0.39
0.66	0.16
0.19	0.05

Value	R1	R2	R3	R4
R1	0.60	0.66	0.54	0.44
R2	0.20	0.22	0.32	0.31
R3	0.12	0.07	0.11	0.19
R4	0.09	0.04	0.04	0.06

Row Sum	Sum/4
2.23	0.56
1.05	0.26
0.49	0.12
0.23	0.06



CBAM

IMPORTANCE

Decision	Performance	Security	Support	Availablity	Versatility	Integrability	Sum
Programming Language	20	25	10	15	20	10	100

RATING [-1, +1] **RISK [0, 1]**

Alternative	Performance	Security	Support	Availablity	Versatility	Integrability	Total Risk	Cost
Python	0.4	0.6	1	1	1	0.7	0.10	$5
Java	0.6	1	0.9	1	1	0.6	0.10	$5
C	1	0.3	-0.1	0.5	1	0.1	0.30	$10

Alternative	Benefit Score	Desireability
Python	70.20	14.04
Java	76.95	15.39
C	40.60	4.06

Programming Language:	Java

IMPORTANCE

Decision	Performance	Security	Modifiability	Availability	Interoperability	Integrability	Sum
Graphics API	20	20	10	10	15	25	100

RATING [-1, +1] **RISK [0, 1]**

Alternative	Performance	Security	Modifiability	Availability	Interoperability	Integrability	Total Risk	Cost
Java SWING	0.1	1	0.4	0.9	0.8	0.9	0.2	$ 10.00
JavaFX	0.5	1	0.5	0.7	1	1	0.3	$ 10.00
AWT	-0.5	1	0.4	1	0.6	0.9	0.1	$ 10.00

Alternative	Benefit Score	Desirability
Java SWING	55.6	5.56
JavaFX	57.4	5.74
AWT	49.95	5.00

Graphics API:	JavaFX

IMPORTANCE

Decision	Performance	Security	Modifiability	Availibility	Interoperability	Integrability	Sum
Primary Input Device	20	30	10	15	10	15	100

RISK [0, 1]

Alternative	Performance	Security	Modifiability	Availibility	Interoperability	Integrability	Total Risk	Cost
Keyboard + Mouse + Touchscreen	1	0	0	0	-0.5	-0.5	0.2	$ 100.00
Keyboard + Mouse	1	0	0	1	1	1	0.1	$ 10.00
Keyboard Only	0.5	0	0	1	1	1	0.1	$ 10.00

Alternative	Benefit Score	Desirability
Keyboard + Mouse + Touchscreen	6	0.06
Keyboard + Mouse	54	5.40
Keyboard Only	45	4.50

Primary Input Device:	Keyboard + Mouse

IMPORTANCE

Decision	Performance	Security	Modifiability	Availibility	Interoperability	Integrability	Sum
Platform	30	30	10	10	10	10	100

RATING [-1, 1] **RISK [0, 1]**

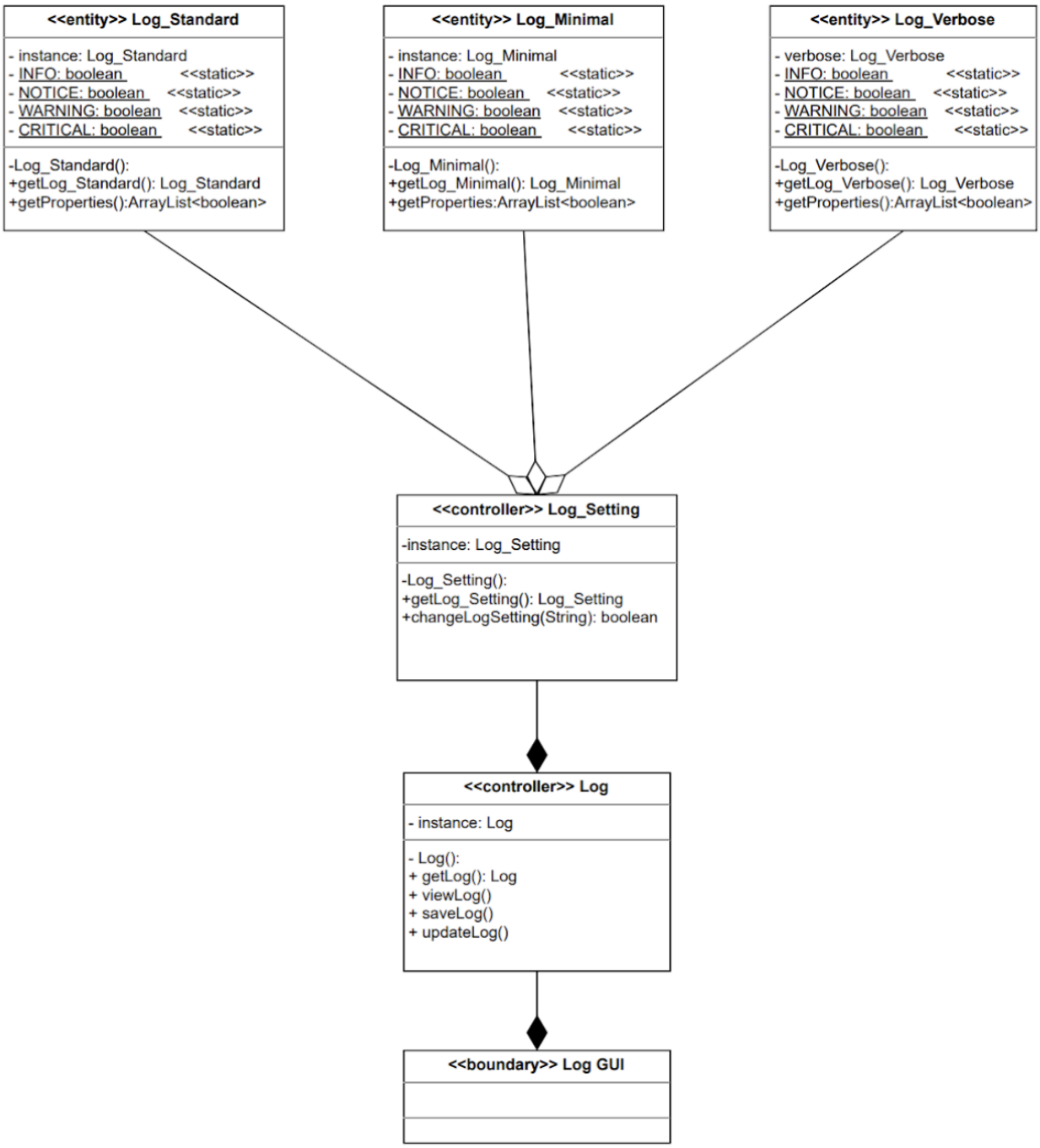
Alternative	Performance	Security	Modifiability	Availability	Interoperabilty	Integrabilty	Total Risk	Cost
Web	0.5	0	1	0.5	0.7	0.7	0.3	$ 100.00
Mobile	0	0.8	0.5	0	0.5	0.5	0.2	$ 50.00
Desktop	1	0.8	0.7	1	0.2	0.8	0.1	$ 20.00

Alternative	Benefit Score	Desirability
Web	30.8	0.31
Mobile	31.2	0.62
Desktop	72.9	3.65

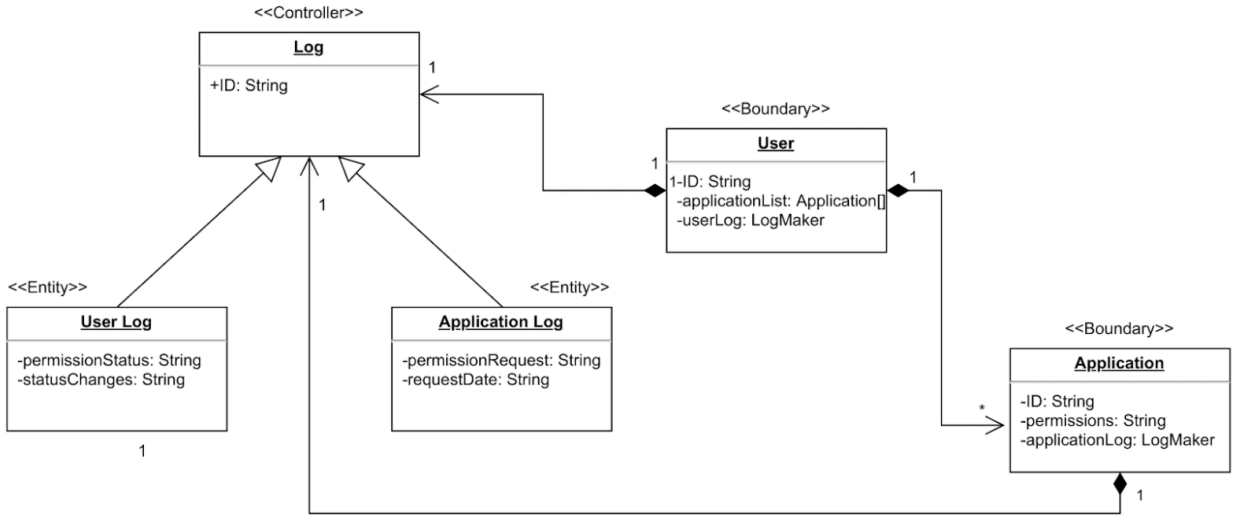
Platform:	Desktop

CLASS DIAGRAMS

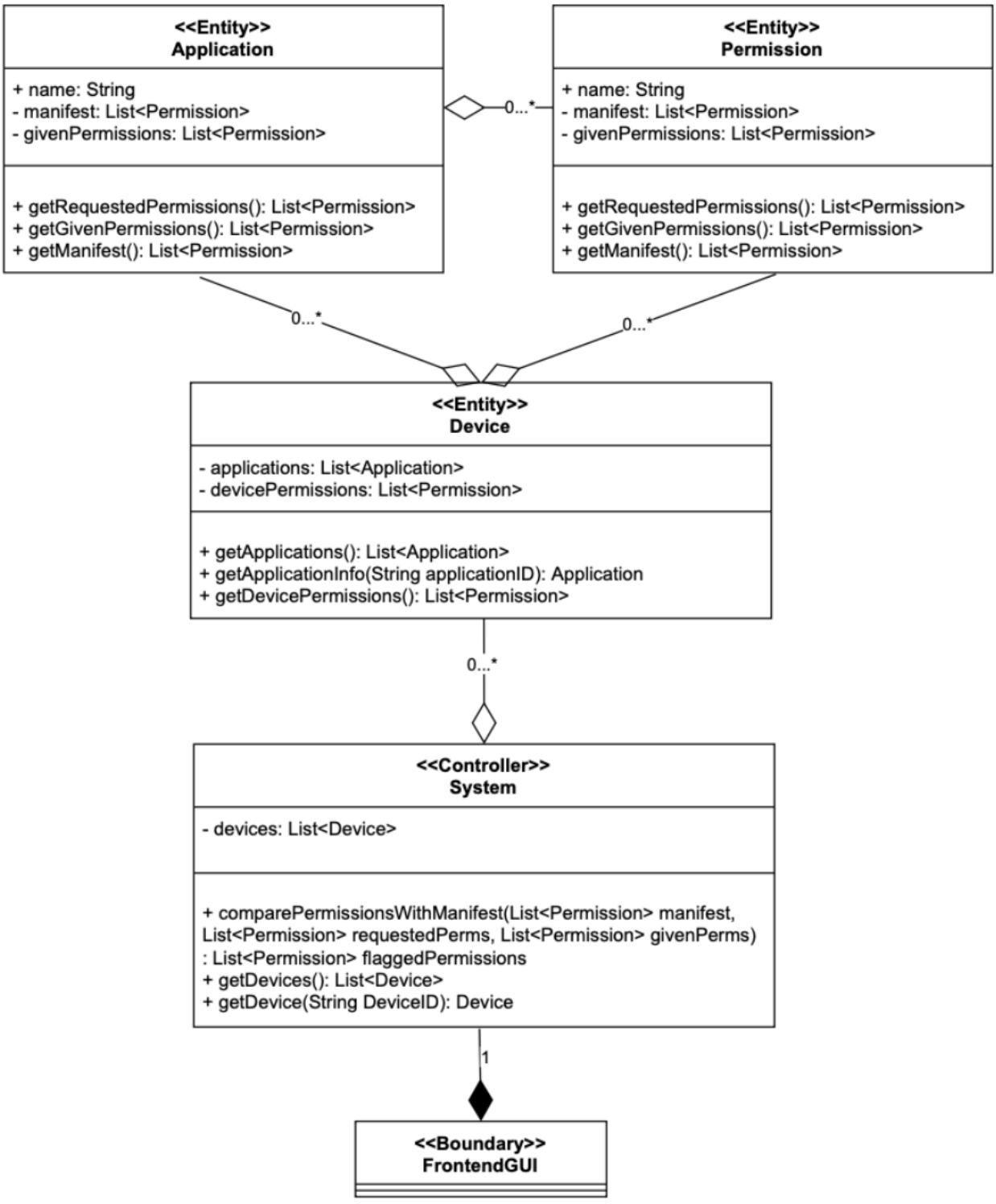
Use Case: Change log settings



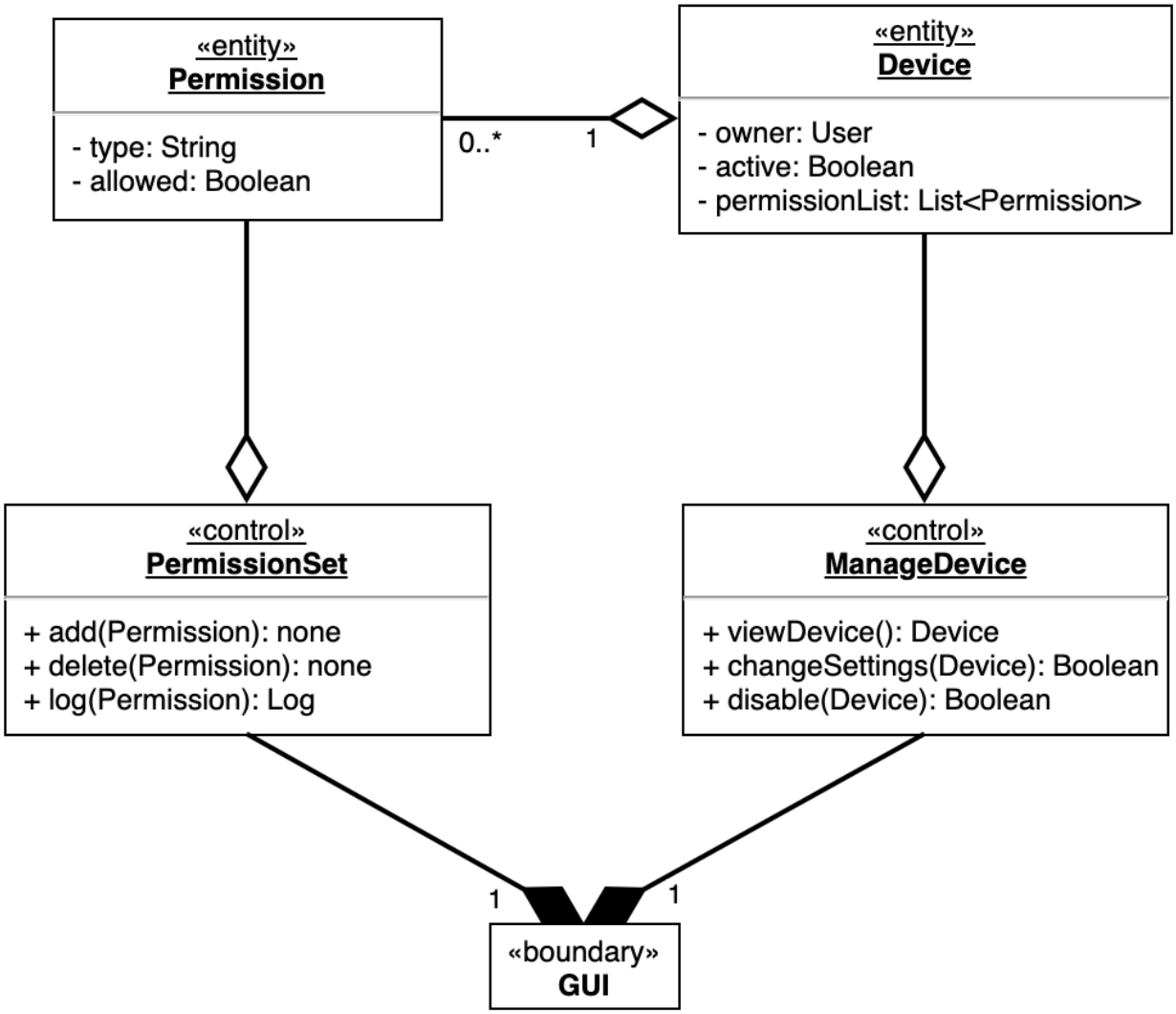
Use Case: Change an application's permissions



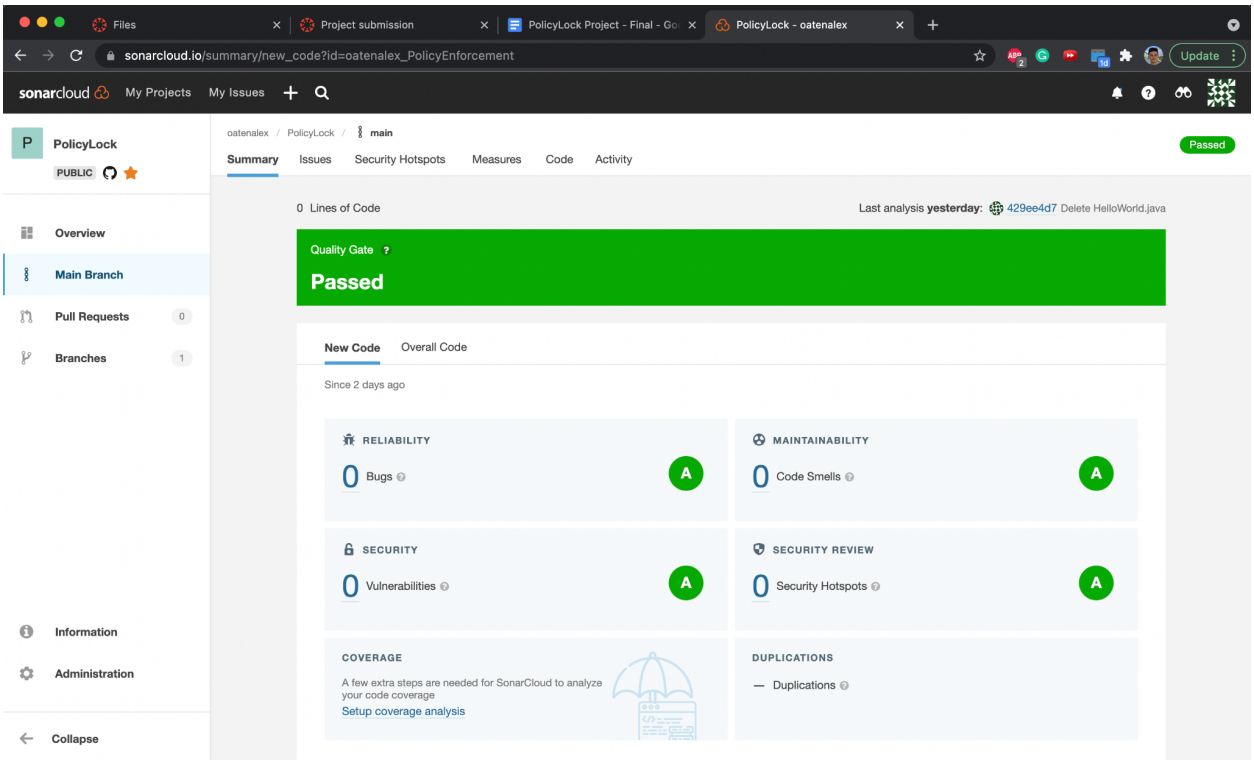
Use Case: Compare given application permissions with manifest



Use Case: Override device permissions



SONARCLOUD



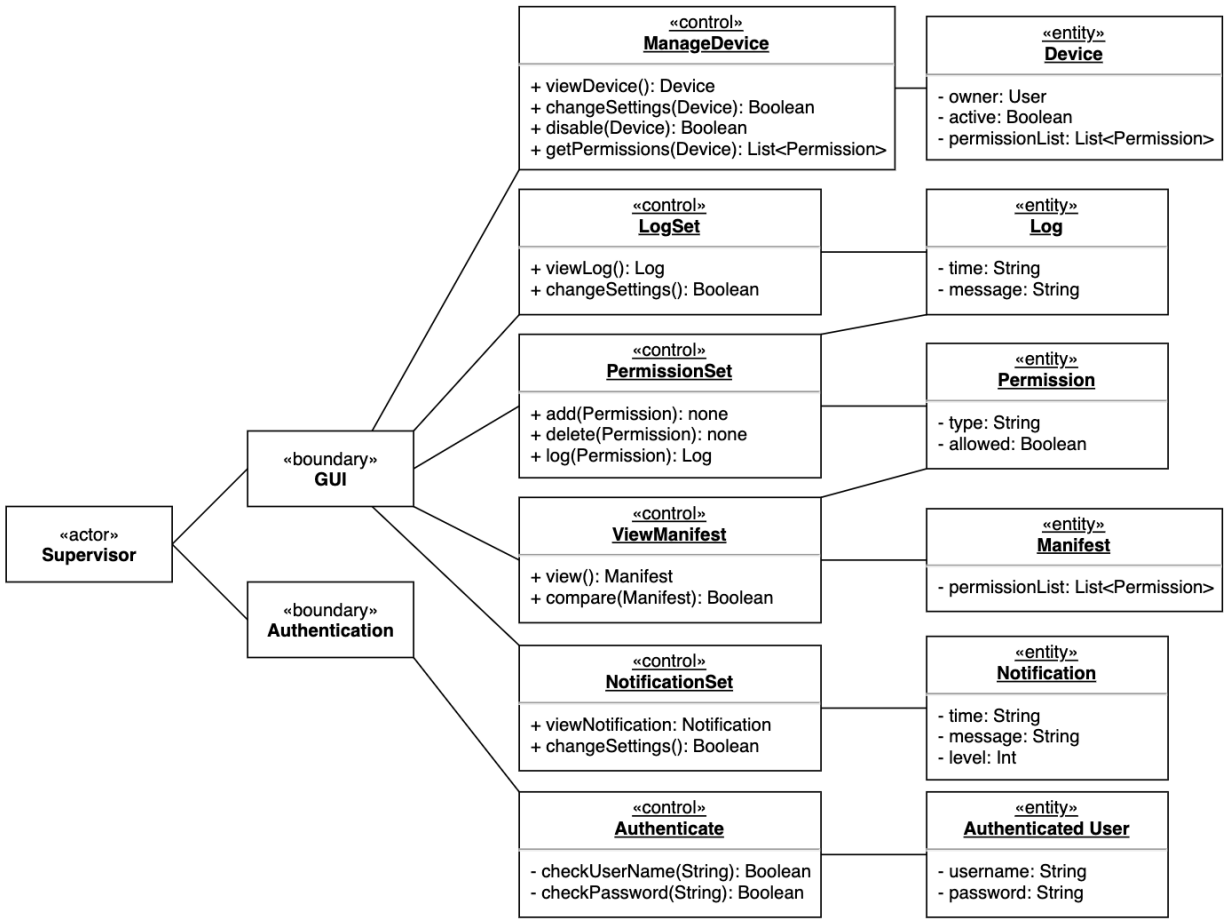
*only about ~1k line analyzed, as most of our code is in .fxml files

[Sonar Cloud Project Link]

[GitHub Project Link]

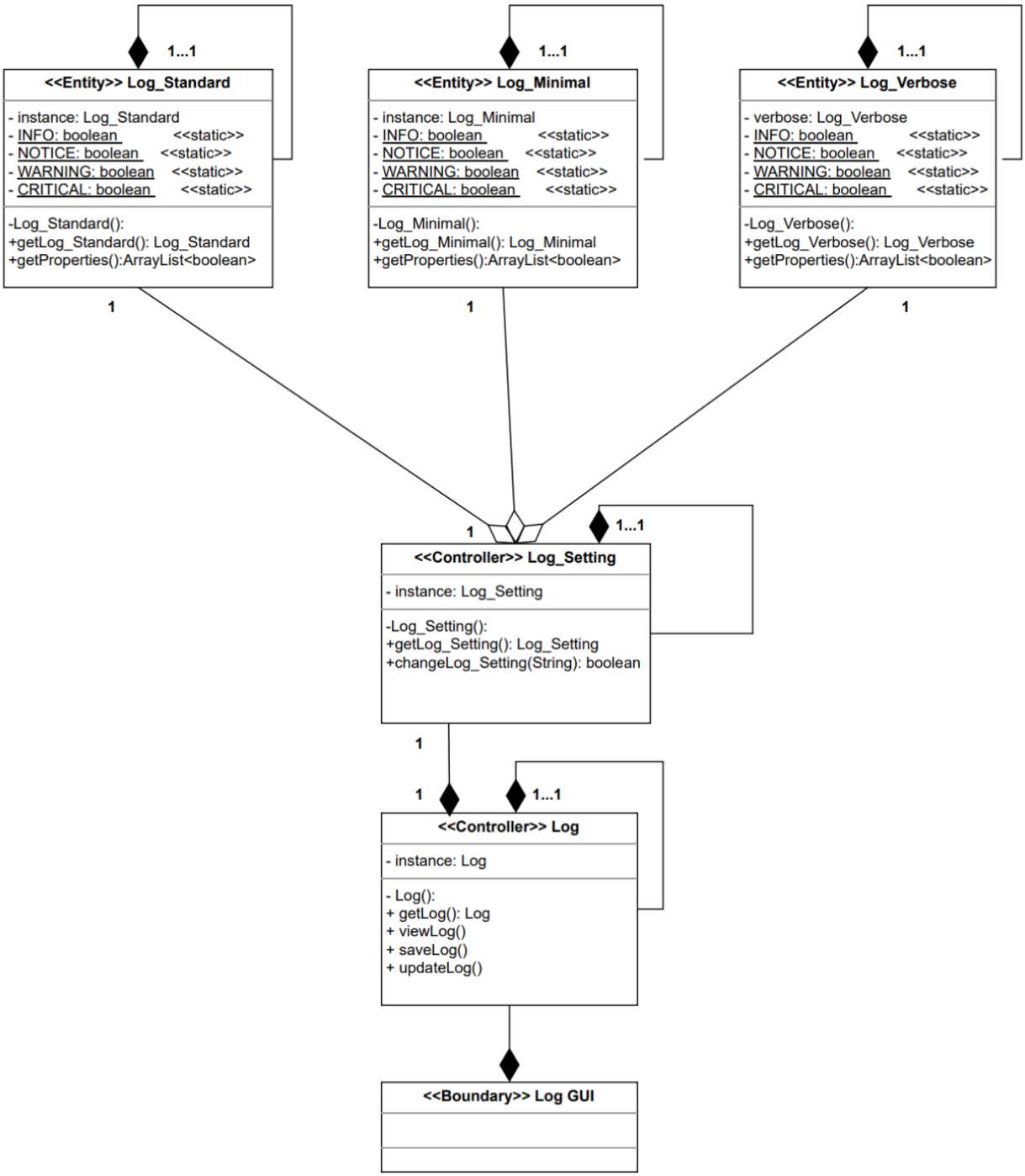
DESIGN PATTERN DIAGRAMS

Design Pattern: Entity Control Boundary



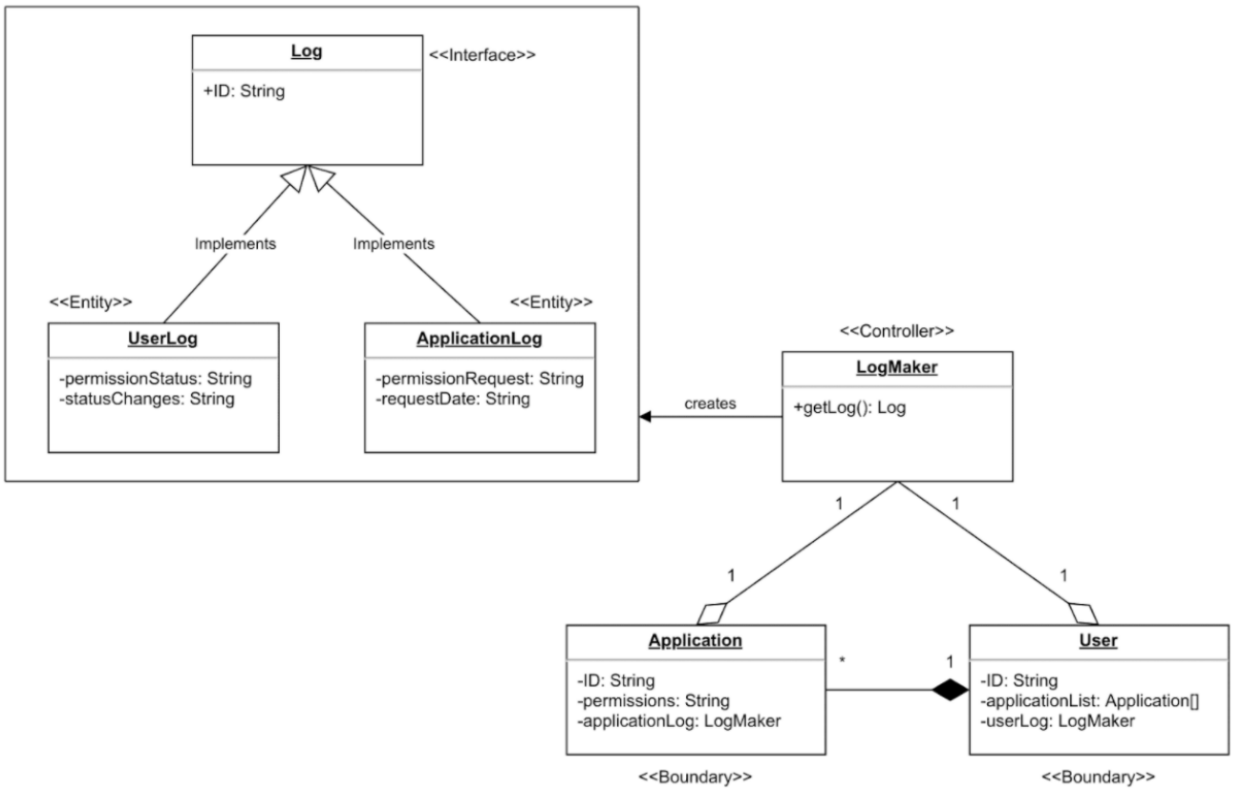
Design Pattern: Singleton

Use Case: Change Log Settings



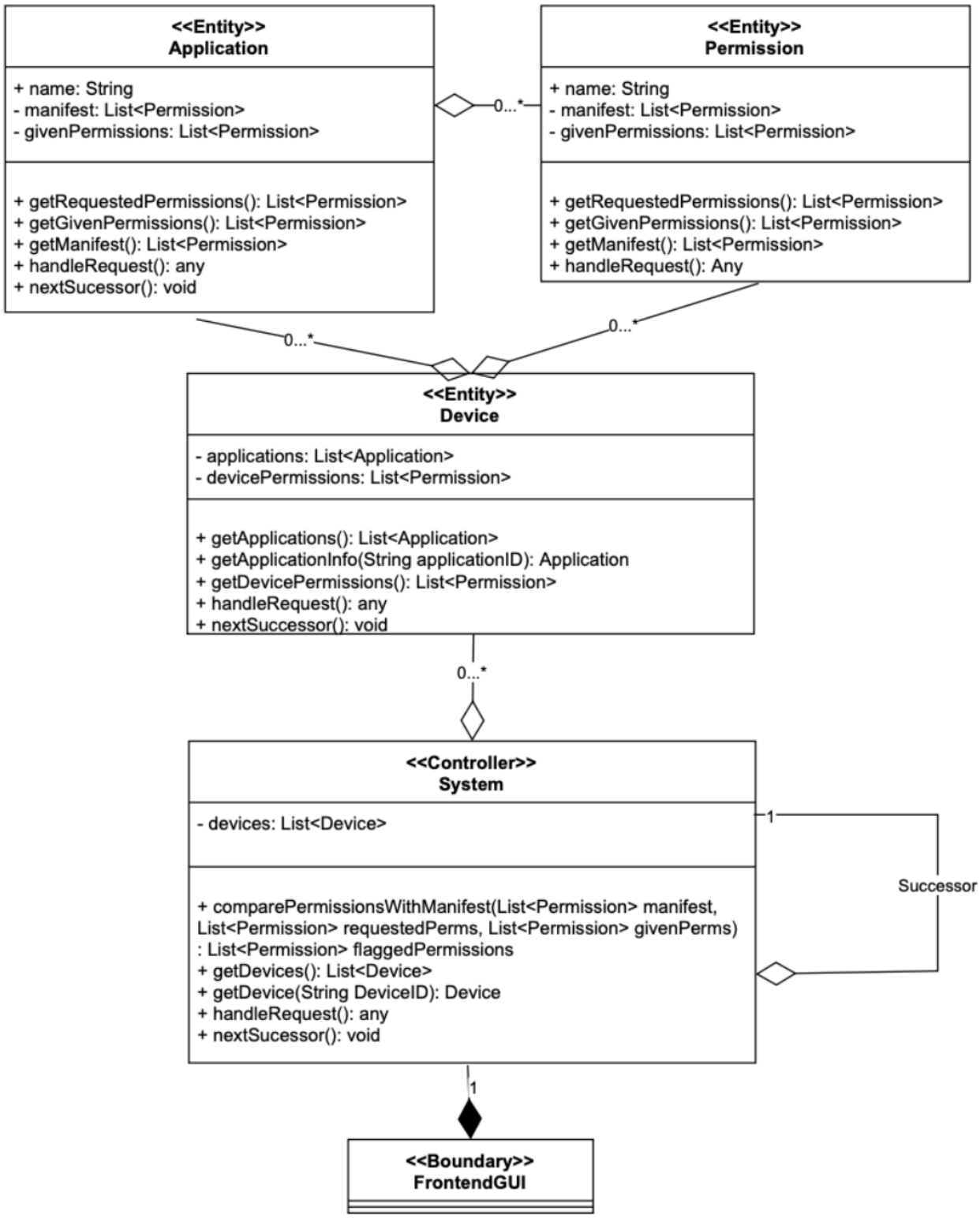
Design Pattern: Factory

Use Case: Change an application's permissions



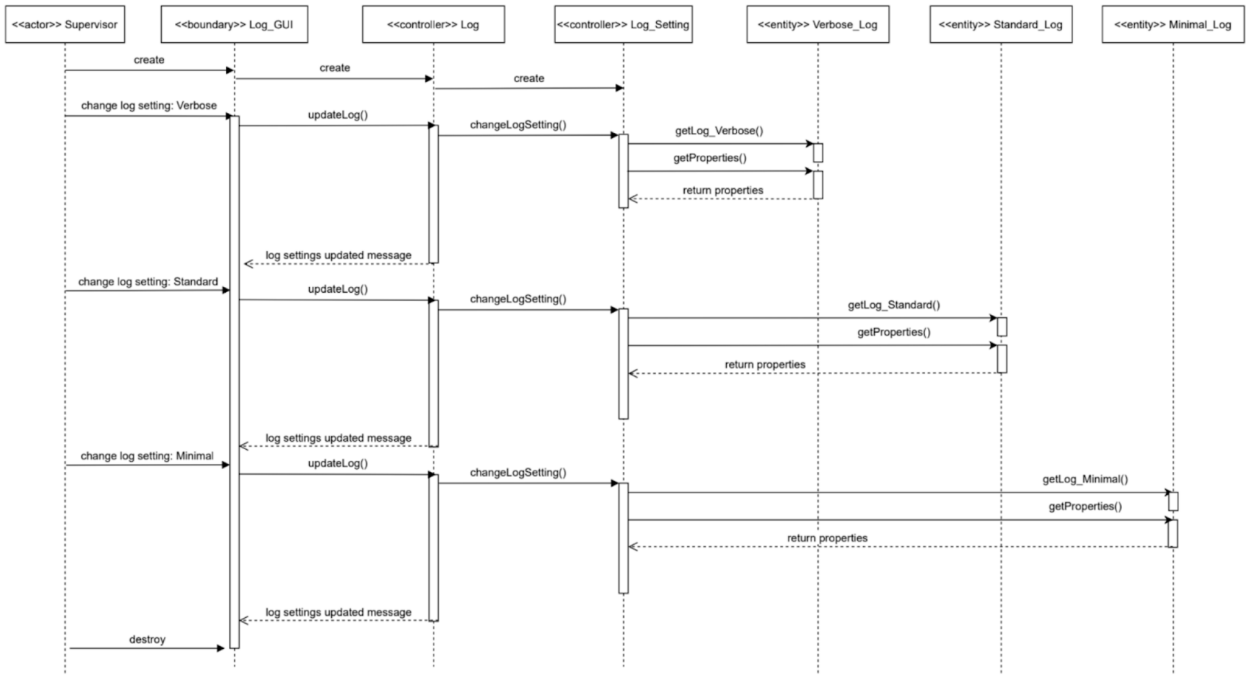
Design Pattern: Chain of Command

Use Case: Compare given application permissions with manifest

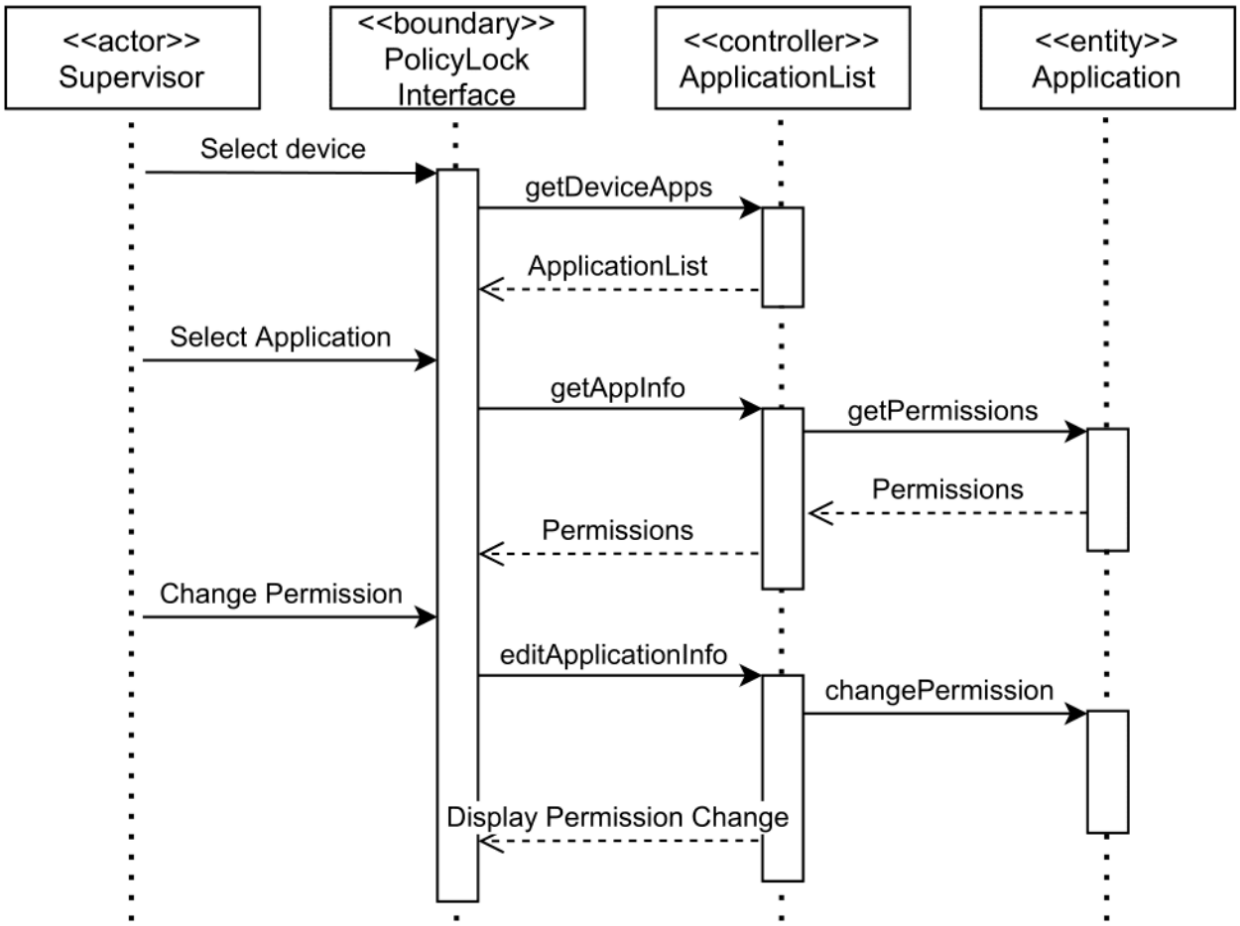

<<Entity>>
Application
+ name: String
- manifest: List<Permission>
- givenPermissions: List<Permission>
+ getRequestedPermissions(): List<Permission>
+ getGivenPermissions(): List<Permission>
+ getManifest(): List<Permission>
+ handleRequest(): any
+ nextSucessor(): void
0...*
<<Entity>>
Permission
+ name: String
- manifest: List<Permission>
- givenPermissions: List<Permission>
+ getRequestedPermissions(): List<Permission>
+ getGivenPermissions(): List<Permission>
+ getManifest(): List<Permission>
+ handleRequest(): Any
0...*
0...*
<<Entity>>
Device
- applications: List<Application>
- devicePermissions: List<Permission>
+ getApplications(): List<Application>
+ getApplicationInfo(String applicationID): Application
+ getDevicePermissions(): List<Permission>
+ handleRequest(): any
+ nextSuccessor(): void
0...*
<<Controller>>
System
- devices: List<Device>
+ comparePermissionsWithManifest(List<Permission> manifest,
List<Permission> requestedPerms, List<Permission> givenPerms)
: List<Permission> flaggedPermissions
+ getDevices(): List<Device>
+ getDevice(String DeviceID): Device
+ handleRequest(): any
+ nextSucessor(): void
1
Successor
1
<<Boundary>>
FrontendGUI

SEQUENCE DIAGRAMS

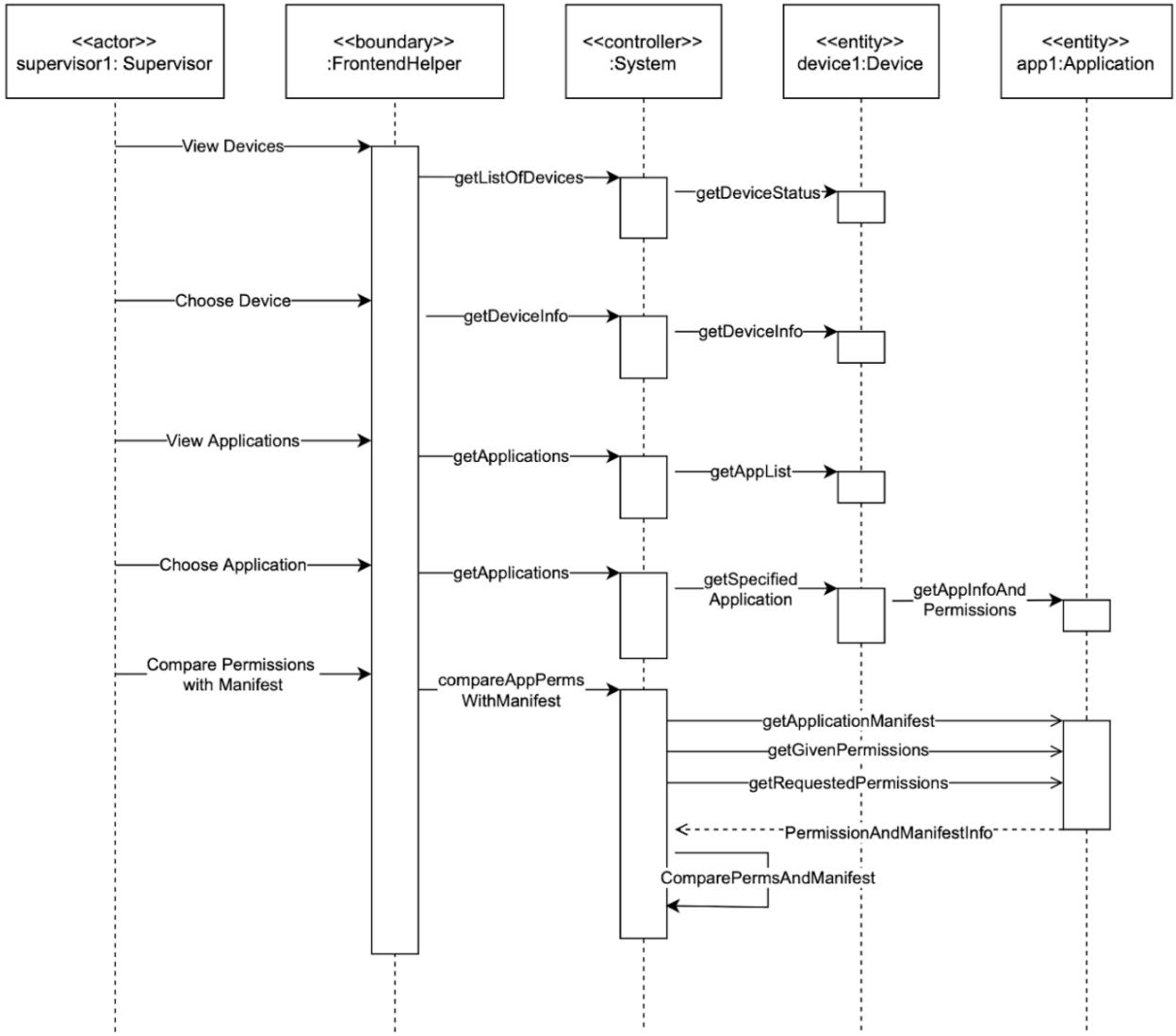
Use Case: Change log settings



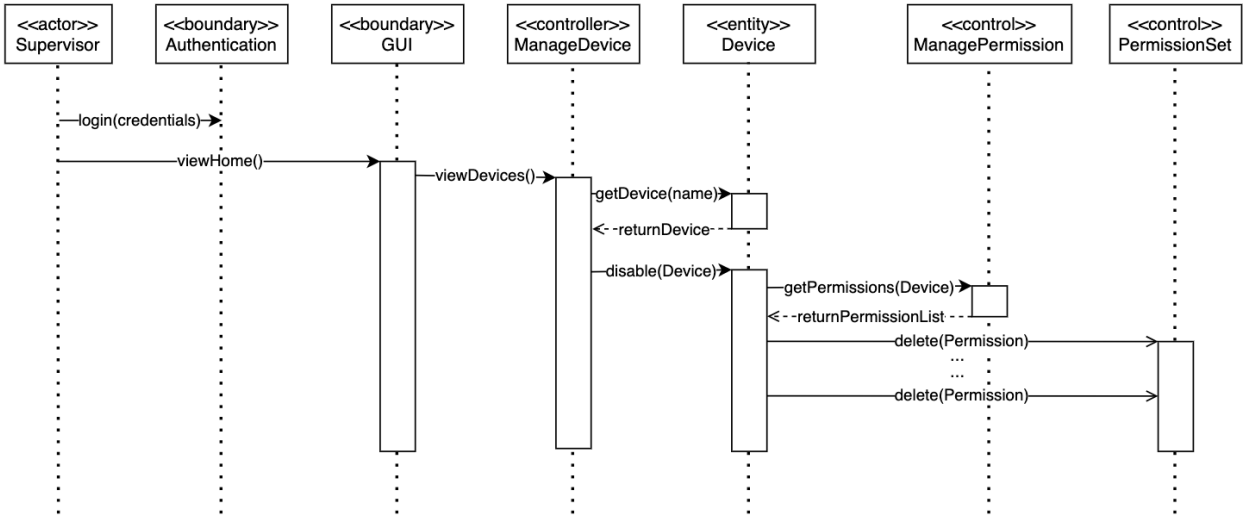
Use Case: Change an application's permissions



Use Case: Compare given application permissions with manifest

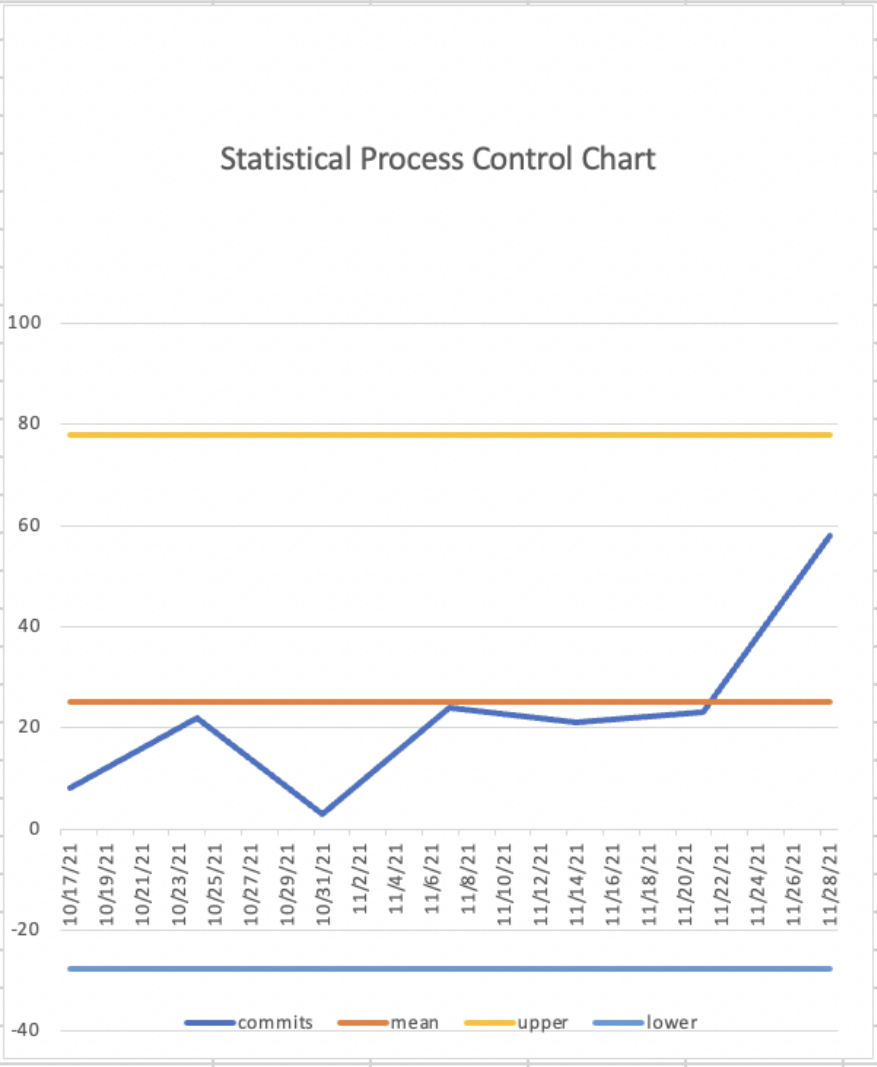


Use Case: Override device permissions



STATISTICAL PROCESS CONTROL CHART

week	commits	mean	sdev	upper	lower
10/17/21	8	25.166667	17.585167	77.922167	-27.588834
10/24/21	22	25.166667	17.585167	77.922167	-27.588834
10/31/21	3	25.166667	17.585167	77.922167	-27.588834
11/7/21	24	25.166667	17.585167	77.922167	-27.588834
11/14/21	21	25.166667	17.585167	77.922167	-27.588834
11/21/21	23	25.166667	17.585167	77.922167	-27.588834
11/28/21	58	25.166667	17.585167	77.922167	-27.588834



ACCEPTANCE TESTING

Name: Login

1. The user opens the application.
2. The system generates the login page. ✅
3. The user enters their username and password.
4. The system verifies the credentials. ✅
5. The system generates the main menu. ✅

Extensions:

4a. *Incorrect username or password & attempts remaining >0.* The system prompts the user to re-enter their username and password, decrements attempts remaining by 1. ✅

4b. *Incorrect username or password & attempts remaining <0.* The system no longer allows the user to attempt to log in. ✅

Use case: View an application's permissions

1. The user logs in.
2. The system displays the home page. ✅
3. The user selects "Devices".
4. The system displays the devices page. ✅
5. The user selects a device.
6. The system displays the applications on the selected device. ✅
7. The user selects an application.
8. The system displays the application's permissions. ✅

Extensions:

6a. *The device has no downloaded applications.* The system displays an empty page. ✅

8a. *The application has no permissions or the permissions cannot be found.* The system displays a message informing the user no permissions could be found. ✅

Name: Change log settings

1. The supervisor logs in.
2. The system displays the main menu. ✅
3. The supervisor opens “Log”.
4. The system opens the log ❌
5. The supervisor opens “Logging Settings”.
6. The system displays current logging settings. ✅
7. The supervisor selects preferred logging setting.
8. The supervisor clicks “Save” button.
9. The system saves the settings and exits back to home.✅

Extensions:

2a. *Database is full:* The system warns the supervisor that the database is full. ❌

5a. *Supervisor has not selected a logging setting*: System prompts supervisor to select a logging setting before they can save and exit. ✅

5b. *Supervisor has selected multiple logging settings*: System prompts supervisor to select only one logging setting before they can save and exit. ✅

Name: Access account management

1. The supervisor logs in. ✅
2. The system displays a home page. ✅
3. The supervisor selects Settings.
4. The system displays a list of settings. ✅
5. The supervisor selects Account Management.
6. The system prompts the user to confirm their credentials. ✅
7. The supervisor inputs their credentials.
8. The system verifies the user’s credentials. ✅
9. The system displays the user’s account settings. ✅

Extensions:

8a. *The user’s credentials are invalid:* The system displays a message saying that the user’s credentials are invalid and prompts them to enter it again. ✅

8b. *The user inputs invalid credentials 3 times:* The system logs the user out. ✅