Detailed Design Review

Liberty Mutual Mobile Authentication Project

4.29.14

Author(s):

Dervasha Buckery, Joseph Delligatti, Patrick Weiler, Denise Dagadu, Kyle McBride

Project Sponsor(s):

Peter Weinhold

IT Enterprise Technology Services. Mobile Solution Delivery

Brian Riley

IT Enterprise Technology Services. Senior Architect

The following document assesses the design approach the project team expects to take throughout the design, development and testing phases of the project, as well as the team's intended final deliverable. The report specified detailed requirements of the project solution as well as providing a low level vision of the solution to the project. The goal of the design review is to understand how the system being developed works, how it is structured, and how it will function.

Table of Contents:

Detailed Design Review (DDR) 2
Design Review Topics: 2
Architecture 3
Activity Diagram 3
Use Case 4
Use Case Narrative 5
Use Case Glossary 5
Network Discussion 7
Network Diagram 9
Security Architecture 9
Standards Compliance 10
System Dependencies 10
Testing Requirements 11
Risks 12
Development Phase 12
Analysis 12
Design 13
Development 13
Unit Test 14
Integration Test 14
Training and Transition 14
Appendix 15
Appendix 1: Activity diagram 15
Appendix 2: User Interface Prototypes 15
Appendix 3.1: STRIDE Risk Assessment 15
Appendix 3.2: FAIR Risk Assessment 18

Detailed Design Review (DDR)

Design Review Topics:

Liberty Mutual Insurance (LMI) is seeking a new approach to two factor mobile authentication to implement within their enterprise. The goal of the Liberty Mutual Mobile Authentication Project as mentioned in the Project Initial Planning Document "is to leverage cell phone mobility to improve traditional IT computing and usability without compromising security". The overall objective is to provide a login system to Liberty Mutual Insurance personnel that creates an environment that is "simple and easy for employees uses of Mobile devices safely and securely". The client has specified that this system should provide a user authentication platform that will:

- Be simple to use for employees
- Can be used by different mobile platforms(IOS, Android)
- Provides multiple levels of authentication

To address the requirements, goals and objectives of LMI and this project, the project team has developed a multifactor mobile authentication solution that uses a combination of fingerprint authentication, short message service (SMS) authentication and an eight digit user enterprise ID provided by LMI to employees. As stated in the project planning document "our team's sponsors are aware that our team may or may not have the resources available and the skills needed to develop and implement this application for all mobile platforms". The final deliverable expected will be design and development documents, functional and structural diagrams related to the developed system and key integrated components, and an illustrative prototype consisting of simple GUIs representing the mobile interface that users would authenticate through. It is the goal of the project team to provide a design solution that can be enhanced to become a functional mobile authentication application that works across different platforms.

Architecture

The authentication system will consist of various components. These components include a standalone application that will act as a hub to connect and interact with the various technologies: a technology known as iFMID, provided by S.I.C. Biometrics, to scan the users fingerprint and an authentication server to leverage SMS and fingerprint authentication.

The iFMID technology provided by S.I.C. Biometrics has both a hardware and software component. The hardware is a fingerprint scanning device that connects to both iPhones and Androids. The software integrates the hardware with a mobile application using an SDK provided by the company. For more specifics on the hardware and software used by the IFMID reader, reference the section titled **Resource Information**.

The authentication server that handles normal authentication of users on personal computers and laptops will also be used to handle the mobile authentication solution. The authentication server will require SMTP to be enabled, and will need an SMS gateways set up for it to communicate with cellular devices. For more specifics on the authentication server, reference the section titled **Resource Information**.

Activity Diagram

The diagram in **Appendix 1** walks through the basic step by step process flow of the mobile authentication application. The system is designed to use a user's fingerprint and an OTP SMS as forms of authentication. An image of the diagram is attached to the document and be viewed there.

The diagram walks through the two different processes the application completes: the first time the user launches the application and enters their information and each time the user launches the application in the future. How the application communicates with the different components does not change, only a couple steps are added in.

After launching, the application will initially check to see if the mobile phone is on Liberty Mutual network, this is a requirement in order to limit the users that can attempt to link the application to their phone but will only occur on the initial installation. The user will then be asked to provide their Liberty Mutual credentials. These are confirmed on the authentication server connected with Liberty Mutual. The credentials will indicate which employee it is trying to link the account so that their information can be pulled later on.

Next, the application checks for the iFMID reader and requests the user to scan their fingerprint. Once scanned, the fingerprint is stored in the authentication server under their credentials. When they return to launch the application, this is the fingerprint that will be compared, to authenticate

the user. Once this is complete, the user will indicate how they would like to receive their OTP via SMS. The authentication server will then send an OTP to the provided information and the user will then enter the received OTP into the application. The entered number is shared with the authentication server which will compare it to the previously sent number and verify the user so that their registration can be completed and they can be logged onto the VPN.

Use Case

The following diagram is a basic breakdown of what the system will be capable of accomplishing. A glossary accompanies the diagram for further explanations.

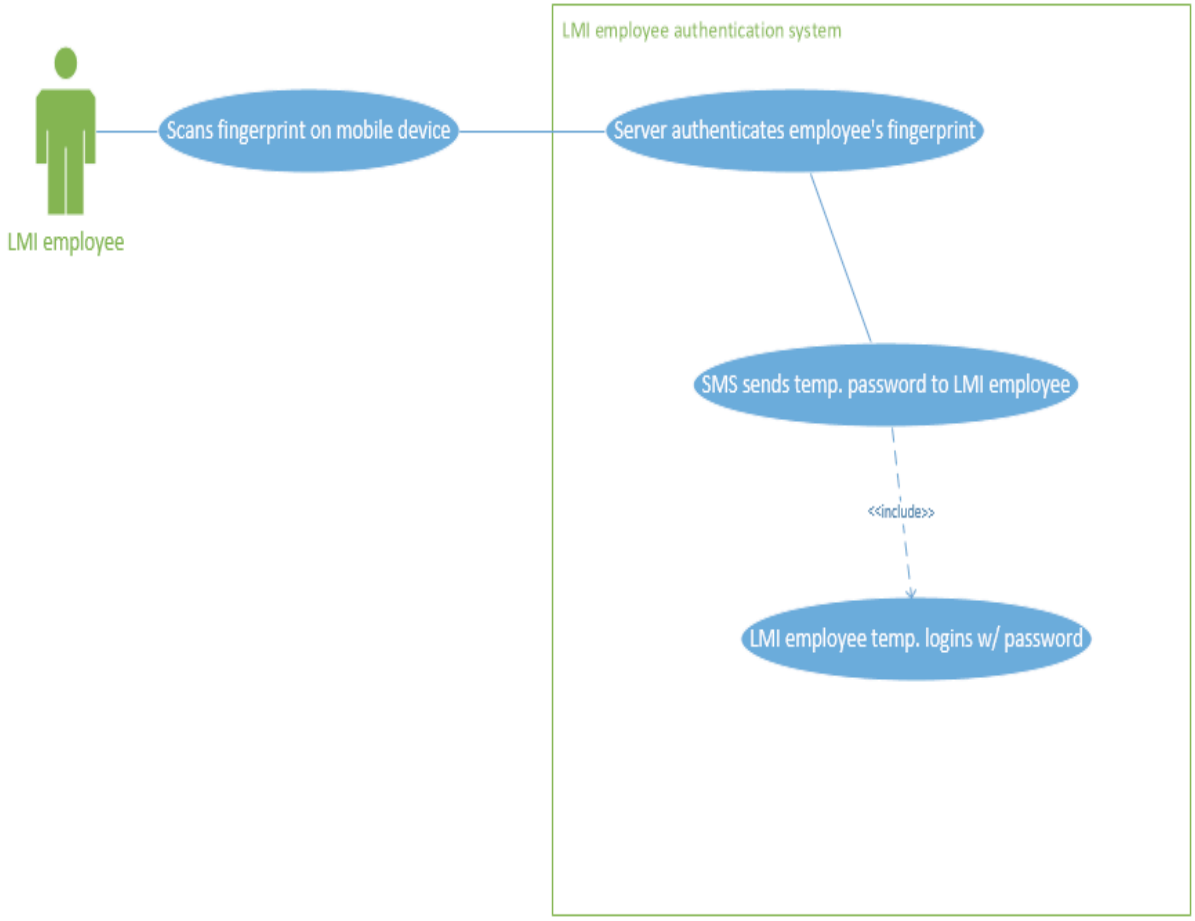


Figure 1: Mobile Multifactor Authentication application Use Case Diagram

Use Case Narrative

The Liberty Mutual Insurance (LMI) Employee scans their fingerprint on their mobile device. Their fingerprint gets stored on a database. Then SMS authentication sends a text message to the employee with his/her temporary password for logging in to the VPN network.

Use Case Glossary

Use Case Name: LMI employee **Brief Description:** This actor is the LMI employee who will be using the mobile authentication system.
Use Case Name: Fingerprint scan **Brief Description:** This is where the employee scans his/her fingerprint on personal device for authentication.
Use Case Name: Server authenticates employee's fingerprint **Brief Description:** provides confirmation that the employee has been authenticate to the SMS server.
Use Case Name: SMS text message **Brief Description:** This is where SMS sends out a text message containing a temporary password for the employee to use in order to login.
Use Case Name: LMI employee login **Brief Description:** This is where the LMI employee logs in with the temporary password given via SMS.

Resource Information

The solution will require the use of a user's or the company's mobile device (smartphones and tablets), the iFMID fingerprint reader, and two authentication servers. Below is more information on the specific resources each piece of technology will require to function.

Mobile Devices (Smartphones, Tablets)
The solution is developed to function on mobile devices which may use different platforms such as iOS for iPhone and iPads and Android OS. The solution requires that the mobile device be compatible with the ability to run an application developed for a mobile platform. The application will require an amount of space on a user's phone to enable it to function; it will not be using or storing any data in the user's phone. The application will communicate with the iFMID fingerprint reader and authentication server.

iFMID Fingerprint Scanner[1]
The iFMID fingerprint reader will be used as an attachment to the mobile device. Once a user accesses the login application on the mobile device, the scanner will be used to collect a user's fingerprint input and relay that data back to the application so it can be compare against the data in the authentication server. The fingerprint reader has the ability to store the fingerprint in three locations: on the mobile device, servers provided by iFMID, and on your own enterprise servers. Our solution will only involve the storing of the fingerprints on an enterprise server. The fingerprints will be stored as an encrypted template file the size of "400 bits" on the authentication server. The reader can scan at least "1000" fingers for up to "20 hours" before needing recharging. Performance of the device is pretty quick; it takes up to two through three seconds to validate a user's fingerprint. The readers will need to be available for employees to sign out as a company resource for use outside of the company.

Servers
One server will be used for authenticating stored fingerprints, authenticating the user's username and sending SMS OTP. The server will require memory to enable it to run through the process of matching the scanned fingerprint with the one on file and storing the OTP passwords. It will also have to be SMTP compatible to enable the OTP to be sent to the user phone. The authentication server receives data from the application and verifies who the OTP should be sent to. This process needs to be available throughout the day, especially during all standard business hours, which predominantly involves the hours of 8am to 6pm. In addition to standard business hours, the process also needs to be available after business hours for employees who need to login at any time and any place, whether they are still in the office or at home.

---

[1] Information about the fingerprint scanner performance and memory requirements can be found on this website: http://www.sic.ca/faq/

Network Discussion

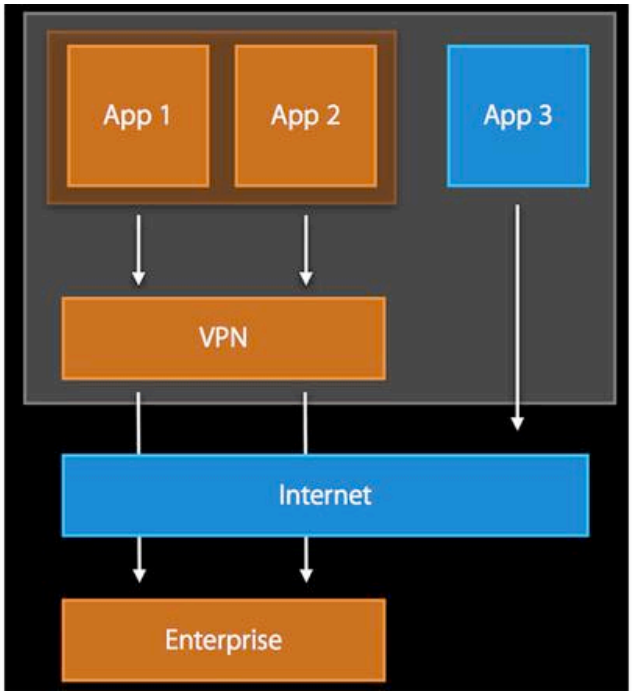
The mobile application will need to communicate with the authentication server in order to provide the user access to Liberty Mutual VPN network. The servers will run on Liberty Mutual Wide Area Network (WAN). Users of the application must have a mobile network or wireless network connection available to them when using the application, the application will need to use that connection to communication with the authentication server. The authentication server can use a wireless network provide by Liberty Mutual or the employee's home network or mobile network(3g 4g) to access the server for validation. On a Wireless network this process can take up to two seconds and on a mobile network provided by a mobile Network provider (AT&T, Verizon, etc.) the process will take up to three seconds. The SMS OTP send from the authentication server may take between a couple of seconds or up to five minutes to be sent to the user's phone. The text will be sent from the server to the user phone through their mobile network provider. It will use the cellular data of the requesting user.

Per app VPN

The application will run using a Per APP VPN environment. This type of environment will protect user information that is sent and received from the application and server. It will also restrict the use of Liberty Mutual VPN network to strictly the authentication application and others applications specified for use on their network. A Per APP VPN configures an application to run in a tunnel when open, all network traffic concerning data being sent or received from that specified application will move through that tunnel. Personal traffic from other applications on a user's phone will be blocked from the tunnel and will not use the VPN connection but will simply connect to the Internet as they normally do through wireless networks or their mobile network (3g, 4g). Liberty Mutual Per App VPN should be managed by Liberty Mutual Mobile Device Management (MDM) System, LMI should specify different rules for devices that connect to their VPN.

Below **Figure 2**[2] illustrates a Per App VPN environment. *App 1* and *App 2* are applications that have been granted access to a VPN, they will use a secure tunnel to access that VPN network and enterprise resources. *App 3* has not been granted VPN access, so it will use its own network connection.

[2] Source: http://www.imore.com/ios-7-what-it-means-enterprise-education-and-government



Dataflow

The flow of data is specified in **Figure 3** below, here are the steps that describe the data flow through the network:

1. The application open and connects to the Per App VPN environment
2. The application collects and reads in the user's fingerprint.
3. It performs a matching process by connecting to the authentication server and checking the file on the server for a match to the inputted fingerprint.
4. When the match is confirmed a message is sent from the server through the SMS gateway to the authentication server. The authentication server, has phone numbers registered for users, the server will find the user's number.
5. The authentication server will generate a one-time password (OTP) for the user and send it to their phone in the form of an SMS.
6. Once the user receives the SMS they will enter their employee issued User-Id and OPT in the application.
7. The application will send this information back to the authentication server, to be checked and authenticate.
8. If accurate the user will be logged into the VPN and given full access.

Network Diagram

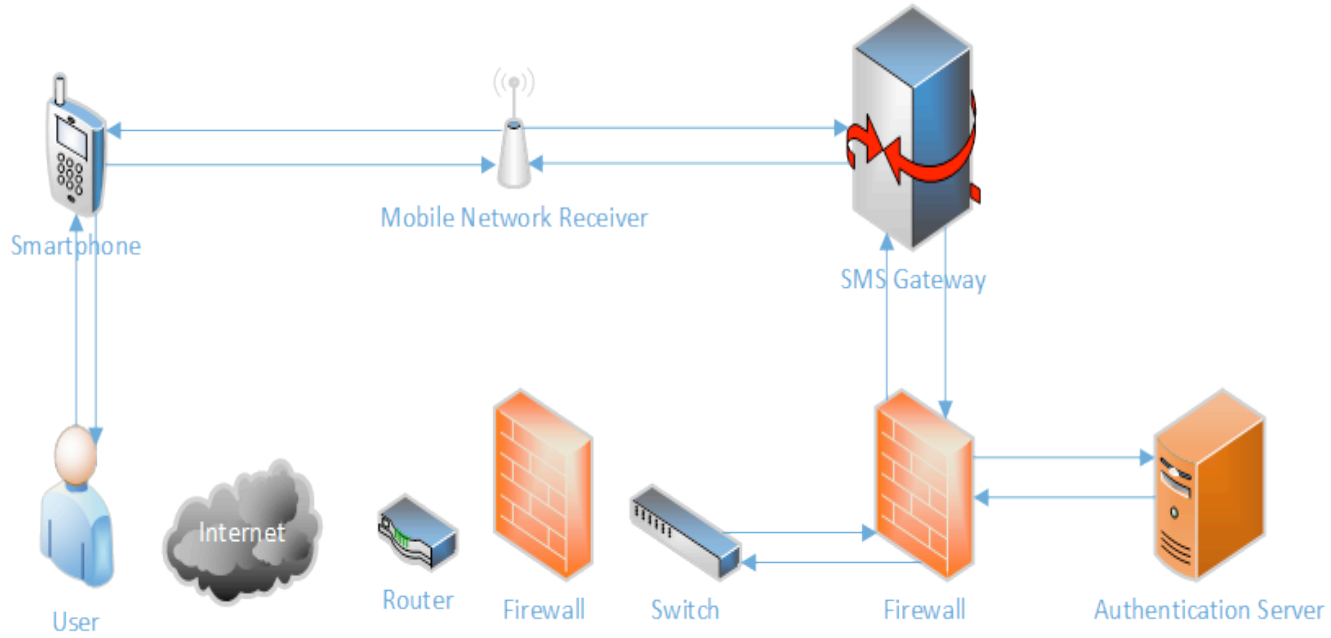


Figure 3: Mobile Multifactor Authentication network diagram

Security Architecture

There are multiple security concerns that factor into the development of an authentication method. The main concerns for this security architecture are impersonation and device management. The strategy that will be used to address these concerns will be to evaluate how these authentication methods uphold the CIA (Confidentiality, Integrity, and Availability) triangle. This will essentially help us isolate vulnerabilities and establish trust level amongst the flow of data from people to technology within the LM enterprise.

One of the techniques used to address these vulnerabilities is the STRIDE Risk Assessment which will highlight the different vulnerabilities associated with spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege. The STRIDE assessment for fingerprint authentication and SMS authentication are included in this report under the *Appendices* 3.1. Also, included within this report is a sample of the FAIR risk assessment in the *Appendices* 3.2. These assessments were conducted so that they could address flaws that may be apparent in current policy. The assessments will provide the Liberty Mutual project clients with the knowledge of each risk that accompanies each authentication factor and way these risks could possibly be monitored with the development or revision of policies that support the mobile work environment within LMI.

Standards Compliance

The goal is for the developed authentication system to be able to effectively manage the risk of an unauthorized user impersonating a Liberty Mutual Employee. Standards of the system all revolve around this goal. The plan is to test against that risk, to assure if impersonation was to take place; the system would be able to combat that. Although the system cannot prevent someone from attempting to impersonate, the multifactorial nature of impersonation should prevent them from getting access to the employee's information through the mobile device. The system will also be tested against the original system requirements to assure that all standards are being addressed. Aside from being able to authorize only respective Liberty Mutual employees, the system must be easy to use. This standard relates to the quality assurance of the system. The system will be assessed against all standards to assure the quality of the developed system. Liberty Mutual requests a system that successfully balances the tradeoff between simplicity and security hence, standards compliance would be a system that effectively addresses this objective.

External Software Requirements

The solution requires the use of the iFMID fingerprint reader software.

iFMID System Development Kit (SDK)
The SDK kit will allow for Liberty Mutual and their development team to have more control over the iFMID readers to incorporate into the authentication application, it allows for "tailor-made identification applications". As the authentication system is to provide ease to the users but still maintain security, it is imperative that Liberty Mutual will have the ability to customize the solution to their needs even when using commercial products as part of the solution. The kit's purpose is to assist in "developing iOS and Android mobile biometric and tailor-made identification applications".[3]

System Dependencies

The authentication application will have three primary functions: a mobile application, SMS functionality and a fingerprint scanning functionality. The application itself requires no specific function from the device that it is operating on, other than the ability to be compatible with the device mobile operating system. The application will depend on the attachable fingerprint reader; therefore the device should also be compatible with the user's mobile device.

[3] Information about the SDK can be found on this website: http://www.sic.ca/sdk-software-development/

The SMS functionality use standard short message service (SMS). The user's mobile device will need to be capable of receiving SMS. This does not include any type of data based messaging system (i.e. iMessage), in the future this may be a possible added function but it will not be a part of the original solution.

The success of the application will be depended on the authentication server; the application will be communicating with, to authenticate users. Users will need to be able to send and receive SMS messages, and the authentication server will need to have an SMS gateway open to accept password requests and to send out OTPs. The server also needs to have SMTP enabled, and needs a custom application running to recognize users and fulfill password requests.

User Interface

The fingerprint scanning application's UI will be very simple and straightforward since its function is so fast and small. It will prompt the user to scan their finger, and display a progress bar so the user knows how long they should hold their finger for to get an accurate scan. The user can leave the application and wait for their password to be delivered via text, or stay in the application and it will notify them that their password has been sent and provide a button to open their default messaging application.

In addition to that, the first time that the user uses the application they will have to take a few extra steps to initiate their phone, their iFMID device and link it with their Liberty Mutual profile. This process is still fairly simple and as said before, will only be done once per device that the user would like to use. The prototype of UI's can be referenced in *Appendices Section 2*.

Testing Requirements

Testing by the project team will be conducted during the developmental phases of the project. The project team plans to test the authentication application in units or segments and gradually work up to a test that contains all units of the application. Testing will be done on both iOS and Android mobile devices since these are the only devices that are supported with the iFMID reader. Further information on testing by the project team can be found in the development section of this document, under the sections Unit testing and Integration Test.

Testing by Liberty Mutual will be conducted in rollout phases by the business unit. LM plans to test all integration aspects of the application with current servers and mobile management services provided by the company. LM will also be conducting user acceptance of the

application. Further information on testing by the LM can be found in the development section of this document under the Training and Transition section.

Risks

A risk assessment plan for all of the possible risks associated with each of the authentication solutions has been compiled. This risk assessment was performed using the STRIDE risk assessment methodology. In addition, a FAIR risk assessment of the authentication factors was performed as well. FAIR risk assessment analyzes the severity of certain risk factors as well as how much money any enterprise can lose due to these risks. See **Appendix 3.1** and **3.2**, for further information on these two assessments.

Advised by the project sponsors, STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of privilege) was the method used to identify risk and threat model, STRIDE is a method first coined by Microsoft to consider threats to computer security.

In addition to the STRIDE analysis, the project team also conducted a FAIR (Factor Analysis of Information Risk) assessment per the request of the project sponsors. The FAIR model was used to identify a variety of threats, possibilities, and outcomes. The method was used to identify which assets were at risk, the possibilities of an attack and how capable attackers were, vulnerabilities, the frequencies of threat events, worst-case and probable losses, and an overall risk calculation. FAIR uses a series of matrices used to calculate the severity of risks, which can range from Very Low to Severe. Similarly to the STRIDE assessment, the FAIR assessment was debriefed with the sponsors who have provided constructive feedback.

Development Phase

Analysis

A significant portion of this project has been dedicated to research. The first few weeks meetings with the project sponsor were dedicated to understanding the problem. Every deliverable is passed by the project sponsor for second opinion. To analyze the problem, research was done on industry trends regarding multifactor authentication. Passwords are still widely used; there was no exact company who could be used as a benchmark on best practices. However, there were multiple scholarly articles on various methods of authentication that were used by the team for reference during research.

From a technical aspect, each option was looked at from four main standpoints ease of use, cost

to implement, security and plausibility of implementation. After possibilities listed, risks of each type of authentication method had to be identified. Advised by the project sponsors, STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of privilege) was the method used to identify risk and threat model, STRIDE is a method first coined by Microsoft to consider threats to computer security. The STRIDE report was debriefed with the project sponsor who then gave constructive feedback.

In addition to the STRIDE analysis, the project team also conducted a FAIR (Factor Analysis of Information Risk) assessment per the request of the project sponsors. The FAIR model was used to identify a variety of threats, possibilities, and outcomes. The method was used to identify which assets were at risk, the possibilities of an attack and how capable attackers were, vulnerabilities, the frequencies of threat events, worst-case and probable losses, and an overall risk calculation. FAIR uses a series of matrices used to calculate the severity of risks, which can range from Very Low to Severe. Similarly to the STRIDE assessment, the FAIR assessment was debriefed with the sponsors who have provided constructive feedback.

Design

The project team will first design the solution through a series of UML diagrams. The system's design will be mapped out through the use of an activity diagram, which will explain the step-by-step flow of the system; a use case diagram and network diagram which will provide a basic breakdown of what this solution is capable of achieving.

The project team discussed at length what the clients were looking for in terms of a final product. Both sides explored several alternatives to producing a working prototype. Since the project team has minimum experience in mobile application development, the proposed final deliverable will be Graphical User Interface (GUI) screens that replicate how intended solution works. The project team will design several GUI screens to demonstrate how the solution will work and each step of the process. The project team will then present these designs to the Liberty Mutual clients.

Development

The development needed for this authentication process will combine a custom solution that integrates licensed hardware/software. The mobile phone will have a custom application to scan fingerprints and then communicate with the authentication servers. The exchange server needs a custom application running to catch requests and recognize users. It then sends off this information to the authentication server, which also needs a custom application for catching, fulfilling, and replying to requests.

Unit Test

The Fingerprint and SMS authentication application prototype will be tested in segments as it is being developed. The authentication functions of the systems which are the fingerprint and SMS will be tested separately to gauge different security risk and functional risk associated with each method. Some of the main risk we will be testing is impersonation and device management. These test will consist of runs to see how well the application can intake user information (phone number, fingerprint) and match it to the database correctly. This test will also be used as an availability and performance test, to address access and speed of the system, results of the test will contain the amount of error produce in each test run.

Integration Test

With the completion of segment testing, the two authentication functions (fingerprint and SMS) will be combined and tested together as a multi factor authentication application. A similar approach to testing method stated in unit test section above will be used to test the authentication of the multifactor application as well as other test that may become significant as the development of the application progresses.

Training and Transition

Training

The project sponsors has requested that training and transitioning current Liberty Mutual (LM) employees from the legacy mobile application system to authentication system developed in this project be conducted by LM. The project team will provide a demonstration to LM to familiarize them with the functionalities of the authentication application. LM will also be provided with recommendations for new guidelines of use for the application which will be the decision of LM to implement in their enterprise.

Transition

LM plans to use the prototype developed by the project team to conduct a rollout phase of test runs within LM. LM plans to start the rollout phase testing with their mobile development business unit and eventually extend it to other business unit within the company. The goal of the rollout test will be to ensure that the authentication application can be effectively used inter-enterprise and also remotely away from Liberty Mutual sites. Liberty Mutual will take responsibility for how the application integrates and operates with their servers.

Appendix

Appendix 1: Activity diagram

Dues to the large size of the diagram it expands throughout multiple pages and would take up too much space in the document. This link leads to the PDF version of the diagram:

https://drive.google.com/file/d/0B0iqKAo5X1zBZzZUUmR4N0JDOXM/edit?usp=sharing

Appendix 2: User Interface Prototypes

Dues to the large size of the UIs it will provided through a PDF. This link leads to the PDF version of the diagram:

https://drive.google.com/file/d/0B0iqKAo5X1zBQkRFelE4T0VBT28/edit?usp=sharing

Appendix 3.1: STRIDE Risk Assessment

Fingerprint Authentication

Fingerprint Authentication is a biometrics authentication method that uses a user fingerprint to identify whether or not they should be authenticated.

Spoofing
Spoofing requires a physical model. In order to replicate the print, the intruder would need to obtain a copy of the users print. The challenge is locating the users print but once located it can be spoofed in a number of ways.

Tampering
Tampering would occur through the phone itself, today most phones are difficult to tamper with unless very specific hardware and software is acquired. Another security application would not increase risk via tampering.

Repudiation
The repudiation of Fingerprint Scanning technology is primarily based off of high advanced the scanner is. Low tech scanners have repudiation. Attackers can replicate a fingerprint with something as simple as a photo. A high tech scanner has little repudiation. Attackers can try and replicated fingerprints but the scanners will recognize that it's not a real finger and deny it even if it's the correct print.

Information Disclosure
Assuming this is the only step to authentication; attackers would only gain access to user information once the fingerprint step was breached.

Denial of Service
A Denial of Service "attack" could occur if the user's finger that they authenticate was damaged. A burn or scratch on the finger may make authenticating difficult. If the device was compromised, the attacker could reset the password to their own finger, and the user would not be able to authenticate.

Elevation of Privilege
If compromised the attacker would be able to gain the privileges made available to that specific user, however elevating above those privileges without any other authentication would not be possible, unless it is allowed to that specific user initially.

SMS Authentication

SMS Authentication is a method of authentication that uses the idea that a user can be authenticated or identified through "something they have". In this case the something the user has is their mobile device which is compatible to receive text based communications. Only after the user has submitted their valid User ID and password (other form of identification: something you know/are) the OTP/token delivered by SMS. To secure the channels that these SMS messages are translated through a common practice, out of band authentication this would use two different channels to send the OTP. Phishing attacks through text messages that trick a user into using a link within the text to enter authentication information could enable spoofing through this technique.

Spoofing

A common attack associated with this method of authentication is the Man in the Middle (MITM) attack. SMS Authentication uses channels to transmit the SMS OTP therefore; the vulnerability to these channels being intercepted is always present. An attacker could possibly trick the mobile user into entering their SMS generated token into a false application. Thereby gaining the token generated by the user. Firewalls and the use of out of band communication should be used to mitigate the risk of MITM attack

Tampering

If a user is able to gain access through a MITM attack or a mobile porting attack there is a possibility that data about the user profile could be tampered with to allow that attack further access to the user account, such as changing of passwords or phone numbers.

Repudiation

This technique of authentication is susceptible to Mobile Number Porting attacks which

according to Wikipedia is when, “an attacker tricks a mobile provider into transferring a victim's mobile number to a new account under the attacker's control. Any SMS messages or calls sent to the victim's mobile number will instead be sent only to the attacker. The victim may be unaware of the attack until the victim notices their cell phone is no longer working, or is no longer assigned the same mobile number”(). Even after this realization the attacker could have switched the mobile service off therefore, leaving no trace of the attacker and no way to prove who was authenticated because the SMS OTP goes to the mobile device associated with the mobile device.

Information Disclosure

Shoulder surfing attacks can be prompted by this attack in the form of a text message notification appearing on an unattended device. It is common for mobile devices to display text message notifications on a device screen, in this case if a SMS OTP is sent to the an unattended device and displayed on the screen an unintentional viewer or attacker could see this information and use it to gain authentication into the device owner account. This can be mitigated by securities policies for device usage that regulate the way notifications are displayed.

Denial of Services

DOS is possible with this authentication method. It can be achieved by an attacker using number porting which will create an interruption or disruption of a mobile device services and ability to receive the SMS OTP for authentication. In addition, a possible denial-of-service attack could be cell tower proximity range. If a user is not within range of a cell tower, the user would not be able to authenticate and login.

Elevation of Privilege

Mobile Number Porting can also be seen as an Elevation of Privilege because it gives an unprivileged user access to authenticate them to an account and possibly compromise user information

Appendix 3.2: FAIR Risk Assessment

Stage 1: Identify Scenario Components

Step 1: Identify the Asset at Risk

At first glance the asset at risk would be the user's mobile authentication device. Looking deeper, the greater threat is what the attacker would have access to. Therefore, the real asset at risk is then the data that can be accessed through that device, along with its intended user because losing possession or control of the device puts the user in a vulnerable state.

Step 2: Identify the Threat Community

The primary threat community for this asset involves humans, and the threat from humans on this asset is both internal and external. It is an internal threat if the owner of the device loses his/her phone/tablet or accidentally damages it, preventing effective login authorization. It is also an external threat in that someone other than the device owner has the potential to steal and/or damage the device if it is left unguarded.

Another internal threat associated with the mobile device comes from malware. Malware has the ability to affect a user's device and can read all of the messages sent to the device. Any user who uploads malware to another user's device will have the ability to read all text messages sent through his/her phone.

Stage 2: Evaluate Loss Event Frequency

Step 3: Threat Event Frequency

This image [4]from the University of Southern California shows that among stolen items in 2013, smart phones are in the "top two" for most stolen item. If you combine that with iPads and other tablets then they are the #1 most at risk personal item on USC Campus. This shows that out of all items stolen, smart phones account for 25% (on USC Campus).

This article by USA Today [5] describes a rise in cellphone related thefts. It includes statements like:
"Nearly half of all robberies in San Francisco this year are cell phone-related" and "more than 40 percent of all robberies now involve cell phones" Said a New York City Police report.

[4] From the University of Southern California: http://capsnet.usc.edu/sites/default/files/all_departments/DPS/Stolen%20Property9S.png

[5]USA Today: http://www.usatoday.com/story/tech/2012/10/20/thefts-of-cell-phones-rise-rapidly-nationwide/1646767/

With this data presented, we would feel confident giving a score of (L) Low for users in large cities. This assumes that at a worst case scenario, their phone will be stolen once per year, but more likely that it would be stolen at least once every ten years..

Step 4: Threat Capability

According to some articles and readings, modern-day thieves are very capable of stealing someone's mobile device, be it cell phone or tablet. The USA Today article mentioned above also details the types of thefts involved, and the type of lengths thieves are going to steal these devices. Now, the article details thefts within the city of San Francisco, so this would be considered a sample of a statistical survey.

According to one section of the article:
"Another robber grabbed an iPhone from an oblivious bus rider — while she was still talking."

The article also mentions that a City Council candidate was robbed at gunpoint for his iPhone. These types of attacks show the potential and capabilities of thieves attempting to steal mobile devices.

Base on this article, it would be safe to assume that the skills and resource ratings can be considered Low (bottom 16%).

Step 5: Control Strength

Without an understanding of LMI's security system, we cannot make a confident assessment of the system's control strength. Still, we feel that it can be rated at Very High (VH). Optimistic of LMI employees, we assume that most of them would keep data on their phone encrypted, and that they would be diligent in warning LMI that their phone had been compromised.

<u>SMS Authentication</u>
Relating to SMS Authentication we feel that the control strength is weak, as the authentication system would not be able to tell who is using the device without the user tipping of the security team that the device was compromised. However, since the attacker would have to get past the fingerprint recognition check first, this could stall the attacker long enough that authenticating through SMS would not be possible. For the SMS authentication on its own though, we would rate it at Moderate (M). This rating is proper because most of the population would be able to send a text that would request a password, but half or less than half of the population would know what to do with it from there.

<u>Fingerprint Authentication</u>
Based on our analysis of fingerprint authentication, we feel that the control strength rating would

be High (H), as in any controls placed on fingerprint recognition would be able to protect against all but the top 16% of the average threat population. An attacker would need to use some rather sophisticated technology to capture a sample of a user's fingerprint. If a fingerprint could be copied through the use of a camera, the camera itself would need to be in very high definition to capture a clear fingerprint.

Step 6: Vulnerability

<u>SMS Authentication</u>

TCap from Step 4: Low
CS from Step 5: Moderate

Tcap \ Vulnerability	VH	VH	VH	H	M
VH	VH	VH	VH	H	M
H	VH	VH	H	M	L
M	VH	H	M	L	VL
L	H	M	L	VL	VL
VL	M	L	VL	VL	VL
	VL	L	M	H	VH

Control Strength

Vulnerability from Matrix above: Low

<u>Fingerprint Recognition</u>

TCap from Step 4: Low
CS from Step 5: High

Tcap	Vulnerability				
VH	VH	VH	VH	H	M
H	VH	VH	H	M	L
M	VH	H	M	L	VL
L	H	M	L	VL	VL
VL	M	L	VL	VL	VL
	VL	L	M	H	VH

Control Strength

Vulnerability from Matrix above: Very Low

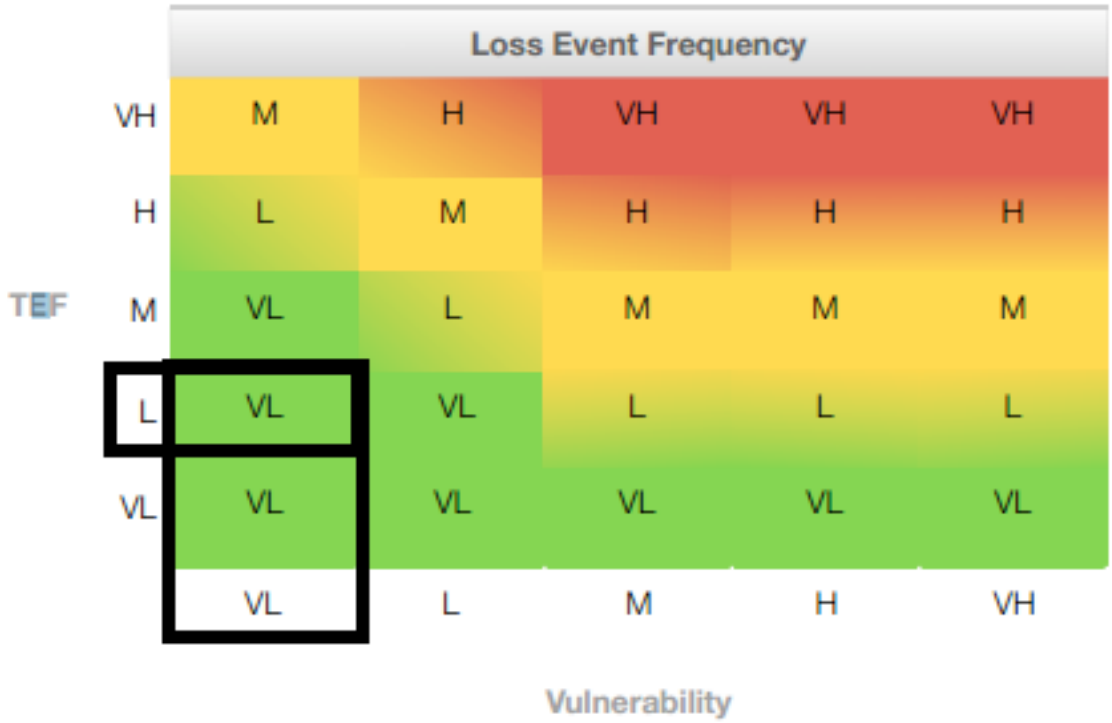
Step 7: Loss Event Frequency

<u>SMS Authentication</u>
Threat Event Frequency from Step 3: Low
Vulnerability from Step 6: Low

TEF	Loss Event Frequency				
VH	M	H	VH	VH	VH
H	L	M	H	H	H
M	VL	L	M	M	M
L	VL	VL	L	L	L
VL	VL	VL	VL	VL	VL
	VL	L	M	H	VH
	Vulnerability				

Loss Event Frequency from Matrix above: Very Low

<u>Fingerprint Recognition</u>
Threat Event Frequency from Step 3: Low
Vulnerability from Step 6: Very Low



Loss Event Frequency from Matrix above: Very low

Stage 3: Evaluate Probable Loss Magnitude

Step 8: Estimate Worst-Case Loss

The following assessment is base on the probability of a LMI employee losing his/her device or having said device being stolen.

Loss Forms

Threat Actions (below)	Productivity	Response	Replacement	Fine/Judgements	Competitive Advantage	Reputation
Access	L	VL	L	VL	M	L
Misuse	L	VL	L	H	SG	M
Disclosure	VL	L	VL	H	H	H
Modification	VL	VL	L	H	H	H
Deny	L	VL	L	VL	M	VL

Access						

The range of Loss is between $7,139,000 and $71,399,970

Step 9: Estimate Probable Loss

The following assessment is base on the probability of a LMI employee losing his/her device or having said device being stolen.

http://fairwiki.riskmanagementinsight.com/?page_id=50

Loss Forms

Threat Actions (below)	Productivity	Response	Replacement	Fine/Judgements	Competitive Advantage	Reputation
Access	VL	VL	VL	VL	L	L
Misuse	VL	VL	VL	L	M	M
Disclosure	VL	L	VL	M	M	M
Modification	VL	VL	M	M	M	M
Deny Access	VL	VL	VL	VL	VL	VL

The range of Loss is between $94,000 and $956,970

Stage 4: Derive and Articulate Risk

Step 10: Derive and Articulate Risk

	Risk				
Severe	H	H	C	C	C
High	M	H	H	C	C
PLM Significant	M	M	H	H	C
Moderate	L	M	M	H	H
Low	L	L	M	M	M
Very Low	L	L	M	M	M
	VL	L	M	H	VH
			LEF		

Loss Event Frequency from Step 7: Very Low
Probable Loss Magnitude from Step 9: Significant
Worst Case Loss Magnitude from Step 8: Severe

Based on the matrix above, this gives us an overall Medium risk level.