Project Plan
Integrated Silent Dynamic Authentication through Symantec VIP
The Capstone Experience

Team Symantec
Scott Binter
Tyler Erskine
James Mariani
Daniel Parlin
Christopher Perry

Department of Computer Science and Engineering
Michigan State University
Fall 2015
Functional Specifications

• Mobile two factor authentication is NOT user friendly
  ▪ Slow and clunky

• Implementation will be fast and seamless
  ▪ No switching applications
  ▪ Embedded
  ▪ Six Digit Authentication Code

• Testing ease of VIP Integration for clients
  ▪ Providing documentation
Design Specifications

• Example implementations
  ▪ iOS
  ▪ Android
  ▪ Web App supporting push notifications

• Seamlessly swap between Symantec VIP enabled applications

• Configurable
  ▪ Fingerprint scanning
  ▪ Timeouts
  ▪ Pins
Screen Mockup: Registration
Screen Mockup: Existing Flow

First Time Accessing Client Application
Screen Mockup: Existing Flow

Subsequent Client Application Accesses
Screen Mockup: ISDA Flow

First Time Accessing Client Application
Screen Mockup: ISDA Flow

Subsequent Client Application Accesses
Screen Mockup: Switching Apps

Subsequent Client Application Accesses
Screen Mockup: Webapp Auth
Screen Mockup: Switching Apps
Technical Specifications

• App Server
  ▪ Linux – Ubuntu 14.04.3
  ▪ Glassfish – 4.1
  ▪ MySQL – 5.5

• Symantec SDK

• App Development Tools
  ▪ iOS - Swift
  ▪ Android - Java

• Web App
  ▪ J2EE
System Architecture

Provisioning a Mobile Credential

1. Sending Username & Pass
2. Validating login info
3. Response
4. Response
5. Request activation code
6. Obtain activation code
7. Activation code to VIP member
8. Send code to phone
9. Obtain shared secret
10. Secret and credential ID sent
11. Register credential ID
12. Add credential ID
13. Response
14. Response

Response credential ID bound to user
System Architecture

Authenticating a Mobile Device

1. Application Server receives Username and password
2. Database queries username and password
3. Application Server confirms user/pass and asks for device code
4. Mobile Application receives "VIP push call" and returns device code for current device
5. Application Server sends VIP device code
6. Application Server requests or returns current device code
7. Verified login complete
System Components

• Hardware Platforms
  ▪ Android Devices
  ▪ iOS Devices
  ▪ Dell Rack Mounted Server

• Software Platforms / Technologies
  ▪ Symantec SDK
  ▪ Linux Server
  ▪ Java/Swift
Testing

• Unit Testing
  ▪ Built into Xcode for iOS application
  ▪ Use Junit for Android and web applications

• User Testing
  ▪ First-time login
  ▪ Regular login
  ▪ Mobile application switching
  ▪ Push notifications for web authentication

• Demonstrations to client
Risks

• Integrating Symantec VIP SDK into our Application
  ▪ Complications may arise during the integration of Symantec’s SDK
  ▪ Refer to provided documentation and request assistance from client

• API Documentation References Older Development Software
  ▪ Provided documentation was written for Eclipse and may not be compatible
  ▪ iOS documented example code written in Objective C
  ▪ Workarounds may need to be found or development software changed

• No iOS experience on team
  ▪ Become familiar with Swift

• Inability to integrate biometric authentication into application
  ▪ Client specified a stretch goal of using biometric authentication
  ▪ Project specifications may have to be adjusted

• No experience with mobile listener services

• Pre-authorized switching between applications