VICTORIA UNIVERSITY OF WELLINGTON
Te Whare Wānanga o te Ūpoko o te Ika a Māui

School of Engineering and Computer Science
Te Kura Mātai Pūkaha, Pūrorohiko

PO Box 600
Wellington
New Zealand

Tel: +64 4 463 5341
Fax: +64 4 463 5045
Internet: office@ecs.vuw.ac.nz

PitchHub - A Collaboration Platform for Innovators

Michael Winton

Supervisor: Dr. Kris Bubendorfer

Submitted in partial fulfilment of the requirements for
ENGR489 - Bachelor of Engineering.

Abstract

The ability to connect innovative ideas to people and resources is an essential component of the innovation process. This project is concerned with empowering the innovation community with an online collaboration system that is simultaneously useful to all actors in the innovation ecosystem while ensuring that all sensitive IP shared is stored in a secure manner. The goal of this report is to detail the steps taken in designing and implementing a distributed web application that facilitates collaboration and enforces data security with threshold cryptography.

Contents

Figures

Chapter 1

Introduction

1.1 Motivation

1.2 Project Objective and Scope

roles and rights (scope of disclosure)

1.3 Contributions

1.4 Outline

Chapter 2

Background into Collaborative Platforms for Innovation

2.1 Common Roles in Innovation

2.2 An Investigation of Innovation-Orientated Collaborative Platforms

2.3 Practical Limitations of Online Collaboration for Innovation

Chapter 3

Background into the Web Application

3.1 Architecture

3.2 Behaviour Driven Development

Chapter 4

Implementation of the Web Application

4.1 Technology Choice

4.2 Deployment

Chapter 5

Background into the Threshold Security Scheme

5.1 Security Considerations

5.2 Shamir's Secret Sharing Scheme

5.3 Limitations of Threshold Security Schemes

Chapter 6

Implementation of the Threshold Security Scheme

6.1 Implementation of Shamir's Secret Sharing Scheme

6.2 Implementation of Secret Keeper Redundancy

Chapter 7

Experimental Methodology

7.1 Functional Testing Method

7.1.1 Testing Environment

talk about reproducible environment

7.1.2 Test Data

frequency analysis of data cleaned and given by CI's user trial

seeded given frequency analysis results

7.1.3 Automated Testing

talk about selenium and user stories

7.1.4 Performance Considerations

talk about NN threshold

7.2 Security Testing Method

7.2.1 Security Testing Scope

Our threat model consists of resisting at least one shoulder surfing attack from an observer co-located at any position around the tabletop. Camera-based attacks are feasible with most knowledge-based authentication systems; but to defeat camera attacks was not our design goal. The pervasive na- ture of mobile devices instrumented with cameras is of par- ticular concern, but as with other manifestations of this same problem (e.g. at the ATM) we rely upon social conventions to deter active attempts to video record logins.

7.2.2 Threat Taxonomy

Chapter 8

Evaluation

8.1 Functionality

8.1.1 Comparison of Prototypes

8.2 Security

8.2.1 Threat Taxonomy

Chapter 9

Summary and Conclusions

9.1 A Summary of The Developed Prototypes

9.2 A Discussion of Online Innovation Collaboration and The Prototypes

9.3 Future Work

9.3.1 Recommendation Engine

9.3.2 Usability Evaluation/Improvement

9.4 Final Comments

Bibliography