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

This chapter aims to explore the related works of collaborative platforms used in the innovation space and also contextualises where in this landscape PitchHub aims to occupy. First, this chapter presents a taxonomy of the primary roles used within the collaborative innovation process. Second, this chapter describes the current collaborative platforms being used in the innovation space and establishes where each stands within the role taxonomy. Third, this chapter concludes with a discussion on the practical limitations that are introduced by being innovation-orientated.

2.1 Innovation Community

In this world of constant communication the creation of ideas is an activity no longer isolated to inventors or researchers. Von Hippel deing innovation communities as "nodes consisting of individuals or firms interconnected by information transfer links which may involve face-to-face, electronic, or other communication" [1]. The world of innovation today now includes actors from increasingly disparate domains where they are able to contribute their unique capabilities to the innovation process [2]. The influx of unique skills being mixed in has resulted in more unique opportunities for innovation being made possible. Therefore to encourage innovation is to also encourage the innovation community as well.

2.2 Common Roles in Innovation

Beyond the uniqueness of the idea, the process of driving an idea from its conceptualisation to its realisation commonly requires a variety of actors who bring together the knowledge, skills and resources required to action its fulfillment [3]. For example, the Apple][came to being with Steve Wozniak providing the technical knowledge and skills, Steve Jobs providing the project goals and marketing drive, and Mike Markulla providing the resources to finance it's production [4]. Again and again we see similar stories, where innovation is driven in a collaborative configuration rather than solely by one person. To this point Callaghan Innovation has identified four distinct roles that are embodied by teams within the innovation process:

- Challenger
- Enabler
- Solver

- Facilitator

These four roles represent the different functions required in an innovative product or service's successful execution. Challengers provide the idea or problem to solved in order to realise a business opporunity. Enablers provide the resources required to action the innovation, this may be in terms of man-power, assets or financing. Solvers provide the answer to the idea or problem presented by the Challenger(s). Facilitators provide the connections to drive the innovation's exection, this may be in terms of connecting other people to the idea, or helping the idea gain reputation. Whether these roles are shared amongst a team or fulfilled by a single person in most cases of innovation these roles are too large for one person to embody them all. To continue with the Apple][example, we may catergorise Steve Jobs as the challenger, asking why computers can't serve the consumer market, Steve Wozniak can be seen as an enabler and sover, as he both designed the Apple][and built them, and Mike Markulla, can be regarded as an enabler and facilitator, as he financed the production and also lent his reputation to the product.

2.3 Innovation Online

One of the key technologies in the modern world is the internet. With the internet, communication and knowledge sharing has never been more accessible or easy. Naturally, the inherenet netowrking that is now a part of the innovation process has been enhanced by the internet and the reach it affords. The increased reach has allowed innovation communities to capitalise on the larger source of innovative potential and knowledge [5].

2.4 Security, Privacy, and Trust in Online Communities

The nature of bringing the innovation process online consequently involves bringing what could be commercially sensitive information online also. In recent times there has been a growing trend of online security attacks where user data has been compromised. Given this reality, there is a large amount of trust involved where users are relying on the platforms they are inputting their sensitive data into to take precautions to keep this data safe. Research in the domain of economics has shown that "without trust, risk is paralyzing; transactions simply do not take place" [6], this notion is similarly applicable in the online innovation space where users are transacting in intellectual property and skills rather than money. This trust enables users to operate in what can be seen as an unsafe environment, where they little power over how the data is stored and who can view it once they have inputted it. It is therefore important for platforms to make good on this trust and implement safeguards against these threats and provide functionality that gives users control of their data.

However, the security of online communities does not solely depend on their technical security. As explored by Johnson et al. in their work regarding Facebook and privacy [7] social networks also face the problem of managing insider threat. Insider threat is where users innappropriately share content with members on the network. This problem is raised by the lack of or under use of privacy controls. In a platform where commercially sensitive information is the content at stake it is important the platform enforce or encourage the use of these privacy controls. A study condcucted by Shin explores the constructs of security, privacy, and trust in social networks, his findings affirmed the above discussion, concluding that security and privacy play vital roles in developing trust from the users [8].

2.5 Related Work

Naturally, a platform that aims to facilitate collaboration for purposes of innovation at it's core is empowering an idea in relation to the roles discussed in Section 2.2. In this section we explore the current solutions being used to facilitate collaboration and discuss how each works in relation to these roles.

IdeaForge [9] is a collaborative innovation platform that supports the Challenger, Enabler and Solver roles. In it's own parlance IdeaForge is described as a three-sided marketplace where users can provide "ideas, time/skills or cash/resources". The main aim for this platform is to facilitate anytime/anywhere collaboration within the global innovation community. Additionally, IdeaForge provides some visibility settings for ideas, where they may be scoped as visible publicly or members only. IdeaForge does not provide functionality for Facilitators, therefore ideas being hosted on IdeaForge require external facilitation. IdeaForge can be regarded as the most similar to PitchHub in spirit as it serves many of the roles identified and provides scoping functionality.

Assembly [10] is a collaborative platform that implicitly supports Challenger, Enabler, Solver, and Facilitator roles. Assembly is orientated around communities that may focus on one or more ideas. The platform does not explicitly distinguish between the roles identified but it's forum-like structure means that any of these roles may raise challenges or solutions within the groups. Assembly's recommender system functionality, where users get recommended groups they may be interested in, illustrates how Assembly itself can be seen as carrying out the Facilitator's role. PitchHub and Assembly differ on focus, where PitchHub focuses on the idea Assembly focuses on the community, this structure while applicable to the innovation space is less directed towards the immediate fulfillment of ideas and more for general collaboration.

AngelList [11] and **Enterprise Angels** [12] are examples of online platforms for investors, a subset of of Enablers, looking to fund businesses. Crowd funding and microequity platforms such as **Kickstarter** [13], **Indiegogo** [14] and **PledgeMe** [15] are becoming increasingly viable sources of funding. These platforms are primarily for Challenger/Solvers looking to seed their innovations, and Enablers looking to get return on their investment. An interesting phenomenon of these platforms is the social "hype" that is sometimes garnered around many of the products/services launched on these platforms. While the solicitation of funds is not a primary goal of PitchHub the inherent socialness of these funding platforms is directly comparable.

Inevitably large social networks have also been used in the innovation space as platforms to help facilitate collaboration. Examples include **LinkedIn** [16] being used by New Zealand Healthcare Innovation [17], **Facebook** [18] being used in the Great New Zealand Science Project [19], and **Google Groups** [20] being used in the National Science Challenges [21]. These platforms have the inherent benefit of convenience as many people in the innovation ecosystem are already members of these networks. These platforms however suffer from lack of (used) privacy controls, and therefore is not a conducive environment for users wishing to discuss commercially sensitive information. These repurposed examples of social networks are in stark constrast to PitchHub's goal of facilitating collaborative innovation.

The proliferation of online networks has been a boon for communities, enabling unprecedented reach. The innovation community has benefitted greatly from these networks, however as demonstrated in the above investigation these networks lack features which serve the directed making of connections between all roles within the innovation community and also lack (used) privacy control functionality.

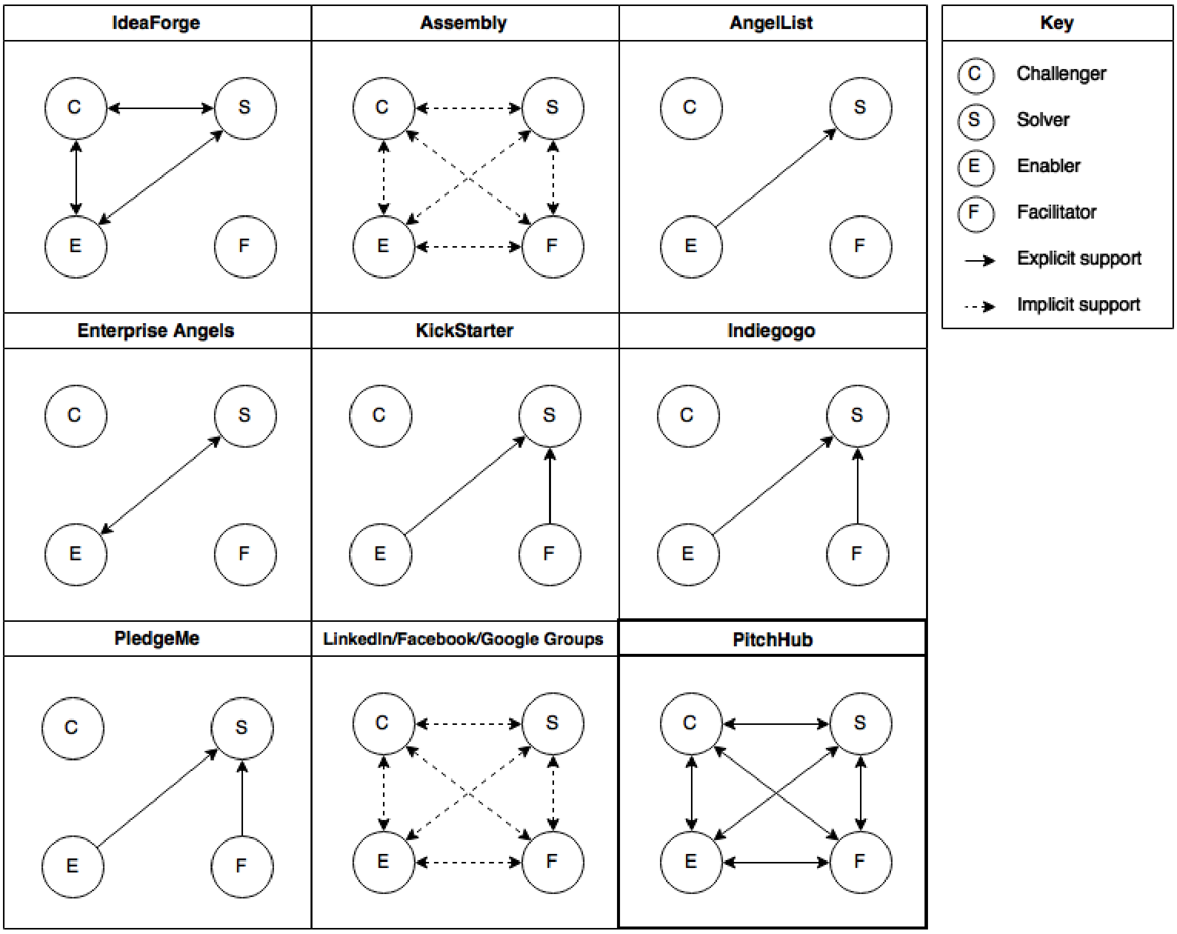

Figure 2.1: All collaborative platforms investigated do not provide explicit functionality for networking between the roles identified in Section 2.2. PitchHub aims to fix this by supporting all roles.

As demonstrated in Figure 2.1 PitchHub seeks to fill the gap in the online innovation collaboration space by being a platform that supports all roles. Throught this PitchHub aims to systematically build valuable business connections centerd around an idea.PitchHub has also been designed to incorporate features from the investigated platform. From FaceBook's privacy control functionality PitchHub extends this with scope of disclosure negotiation, this is discussed later in Section ???.

2.6 Database Security

Securely storing data is a large and increasingly important research area to modern society. In recent years companies like Sony, Apple and Adobe have experienced data breaches resulting in compromised user data. In a system like PitchHub where commercially sensitive information is being handled extreme care must be taken to ensure its safety.

2.6.1 Threshold Security Schemes

Secret Sharing schemes are a type of Threshold Security Scheme where a piece of data is split into n secret shares. To retrieve the original data a threshold of k of n shares (″k, n″) must be met before the original piece of data can be decrypted. A fictional scenario that describes this concept is where the code for launching a nuclear missile is split between three officers, to launch the missile all three officers must be present to reconstruct the launch code. Each share in isolation cannot be used to launch the missile, nor can it be used to infer the original code. This ″3, 3″ example is somewhat contrived but it showcases the fundamentals of secret sharing in that: the secret can be recovered given the threshold is met and the secret is indeed secret when any combination of t shares are less than k.

2.6.2 Threshold Security Schemes

Shamir′s secret sharing [22] is a threshold scheme based on polynomial interpolation.

$$q(x) = a_o + a_1 x + ... + a_{k-1} x^{k-1}$$

The fundamental idea is that given a ″k, n″ scheme a random polynomial of degree k-1 may be generated where the secret D is hidden as term a_o. A set of n points may then be constructed from this polynomial and shared to n secret keepers. To recover the secret D the process requires a subset of k secret shares to calculate the coefficients of the polynomial using interpolation. With this a system is able to recover the secret D at term a_o.

Shamir′s Secret Sharing scheme effectively allows a system to share secrets to n secret keepers while maintaining each secret′s safety as a long as a threshold of k malicious secret keepers is not met. Besides being secure, Shamir′s Secret Sharing scheme holds a number of other useful properties such as being minimal, extensible and dynamic [22]. The scheme is minimal in that the the size of each share does not exceed the size of the original secret. The scheme is extensible in that n may be increased by giving new secret keepers new points from the polynomial. The scheme is dynamic in that the shares may be changed by modifying the polynomial but retaining the term a_o.

As discussed in a number studies the simplicity of Shamir′s Secret Sharing scheme does present limitations that have the potential for being exploited [23][24]. First, complete trust is given to the system who is dealing the secret shares, if an error occurs the secret may be irrecoverable therefore the system dealing the shares can be seen as a single point of failure. Second, Shamir′s Secret Sharing scheme cannot detect secret keepers that cheat by supplying wrong shares, this brings about the problem where if k members are compromised not only will the secrets be recoverable by the malicious party but the compromised members may be used to supply wrong secret shares to the system, effectively denying the first party system of recovering secrets. To combat these exploits Shamir′s Secret Sharing may be extended with signature schemes [25][26] and verification schemes that do not assume the party dealing the shares is honest or infallible [27][28].

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

[1] E. A. Von Hippel, “Democratizing innovation,” 2005.

[2] Y.-K. Che and I. Gale, “Optimal design of research contests,” *The American Economic Review*, vol. 93, no. 3, pp. 646–671, 2003.

[3] J. F. Engelberger, “Robotics in practice: Future capabilities,” *Electronic Servicing & Technology magazine*, 1982.

[4] J. Livingston, *Founders at work: stories of startups' early days*. Apress, 2007.

[5] J. Hautz, K. Hutter, J. Füller, K. Matzler, and M. Rieger, “How to establish an online innovation community? the role of users and their innovative content,” in *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*. IEEE, 2010, pp. 1–11.

[6] J. Boyd, “In community we trust: Online security communication at ebay,” *Journal of Computer-Mediated Communication*, vol. 7, no. 3, pp. 0–0, 2002.

[7] M. Johnson, S. Egelman, and S. M. Bellovin, “Facebook and privacy: it's complicated,” in *Proceedings of the eighth symposium on usable privacy and security*. ACM, 2012, p. 9.

[8] D.-H. Shin, “The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption,” *Interacting with Computers*, vol. 22, no. 5, pp. 428–438, 2010.

[9] “ideaforge — the new engine of creation,” http://ideaforge.io/, (Visited on 08/24/2015).

[10] “Assembly,” https://assembly.com/, (Visited on 08/24/2015).

[11] “Angel list,” https://angel.co, (Visited on 04/07/2015).

[12] “Enterprise angels —startup capital—entreprenuers—angel fund,” http://www.enterpriseangels.co.nz/, (Visited on 08/26/2015).

[13] “Kickstarter,” https://www.kickstarter.com/, (Visited on 08/26/2015).

[14] “Indiegogo: The largest global crowdfunding & fundraising site online,” https://www.indiegogo.com/, (Visited on 08/26/2015).

[15] “Pledgeme,” https://www.pledgeme.co.nz, (Visited on 04/07/2015).

[16] “Linkedin,” https://www.linkedin.com, (Visited on 04/07/2015).

[17] “New zealand healthcare innovation — linkedin,” https://www.linkedin.com/groups/New-Zealand-Healthcare-Innovation-2035021/about?report%2Esuccess=8QK6tymVv4FNpt6BxhCPZkDgzjfC-GH21u7zSpGeVjkNQ3hCQIv-c5Ggp8y0Zj2hqdM4ZJcgV2MPLXh (Visited on 08/26/2015).

[18] "Facebook - log in or sign up," https://www.facebook.com/, (Visited on 08/26/2015).

[19] "The great new zealand science project — facebook," https://www.facebook.com/nzscience?ref=ts&fref=ts, (Visited on 08/26/2015).

[20] Google, "Google groups," https://groups.google.com/forum/#!overview, (Visited on 04/07/2015).

[21] "Nz nsc 10 science for technological innovation - google groups," https://groups.google.com/forum/#!forum/nsc10, (Visited on 08/26/2015).

[22] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[23] A. Abdallah and M. Salleh, "Analysis and comparison the security and performance of secret sharing schemes," *Asian Journal of Information Technology*, vol. 14, no. 2, pp. 74–83, 2015.

[24] J. L. Dautrich and C. V. Ravishankar, "Security limitations of using secret sharing for data outsourcing," in *Data and Applications Security and Privacy XXVI*. Springer, 2012, pp. 145–160.

[25] V. Shoup, "Practical threshold signatures," in *Advances in CryptologyEUROCRYPT 2000*. Springer, 2000, pp. 207–220.

[26] M. Abdalla, S. Miner, and C. Namprempre, "Forward-secure threshold signature schemes," in *Topics in CryptologyCT-RSA 2001*. Springer, 2001, pp. 441–456.

[27] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung, "Proactive secret sharing or: How to cope with perpetual leakage," in *Advances in CryptologyCRYPT095*. Springer, 1995, pp. 339–352.

[28] C. Cachin, K. Kursawe, A. Lysyanskaya, and R. Strobl, "Asynchronous verifiable secret sharing and proactive cryptosystems," in *Proceedings of the 9th ACM conference on Computer and communications security*. ACM, 2002, pp. 88–97.