minicure.

Where security lies in you.

Submitted to: Mediacorp
Company: Square Inc.
Date: 15 October 2016

Prepared by: Chua Kim Hong, Ashley (Ms.)
Tan Qing Yang (Mr.)

Executive Summary

The Internet is an enabling medium for businesses to conduct quick online transactions, including internet banking (iBanking) service which the banking industry has adopted to provide users with services akin to making a trip down to the bank. However, the current adoption of iBanking is flawed as there are several pressing issues that needs to be addressed.

1. Malware threats: exposing users' bank account to theft
2. Inconvenience of owning multiple tokens: limiting the fundamental use of iBanking
3. Recurring US$6,500,000: replacement and environmental cost per annum

To tackle these issues, we engineered a technological solution – Minicure, which incorporates the use of Information Technology and Engineering to offer the following:

1. New Security System
2. Unparalleled Convenience
3. High Cost-efficiency

Minicure promises a return of investment of 14.9%. Relevantly, it provides a practical security system that would safeguard your investment money holding in banks; otherwise be vulnerable to security threats.

Table of Contents

1 Introduction

Prevalent malware security threats are constantly growing, targeting various technological platforms. Sophisticated Trojan has evolved, now owning the capability of keylogging and stealing user's password (Wueest, 2016).

iBanking[1] is the most susceptible to malware attacks as it concerns potential monetary loss for both consumers and service providers. iBanking uses Two Factor Authentication[2] (2FA) as a security countermeasure which provides an added layer of security, but it is fundamentally flawed within.

Responding to Mediacorp's call for business plan, we mined the pressing problems embedded in the current security system of iBanking, supported with market research. The buildup would establish the grounds for a need to call for a comprehensive solution - Minicure.

[1] iBanking is refers to the electronic payment system

[2] 2FA refers to the use of two out of the following three authentication factors:
1. The knowledge factor: knowledge of password, pin or pattern.
2. The possession factor: Owning a security token, Automated Teller Machine card or SMS verification code.
3. The inheritance factor: biometrically verified via fingerprint or retina scan.

2 PROBLEMS

The current 2FA security system has a multitude of trailing problems ranging from the vulnerability to malware threats to the financial and environmental costs of existing tokens.

2.1 Malware threats

Users have regarded the usage of soft tokens via Short Message Service (SMS) one-time password (OTP) as their choice of verification for 2FA, oblivious to the threats of malware attack for perpetrators against Global System for Mobile Communications (GSM) and 3G/4G networks. As there is no added layer of encryption to SMS transmission, OTP can be intercepted and snooped during transmission; generated without the user's intent and diverted to a specific source. Consequently, the soft tokens must not be the dependent solution for 2FA (Hummer, 2016).

In addition, security threats are not limited to soft tokens. Hard tokens which banks have prided as a superior 2FA have been reported to be vulnerable to malware attacks. As the use of existing hard tokens does not require any authentication, perpetrators have the ability to insert malware at the token's infrastructure to exploit the authentication server, masquerading as the user (Baker, Filipiak and Timlin, n.d).

2.2 Inconvenience of owning multiple tokens

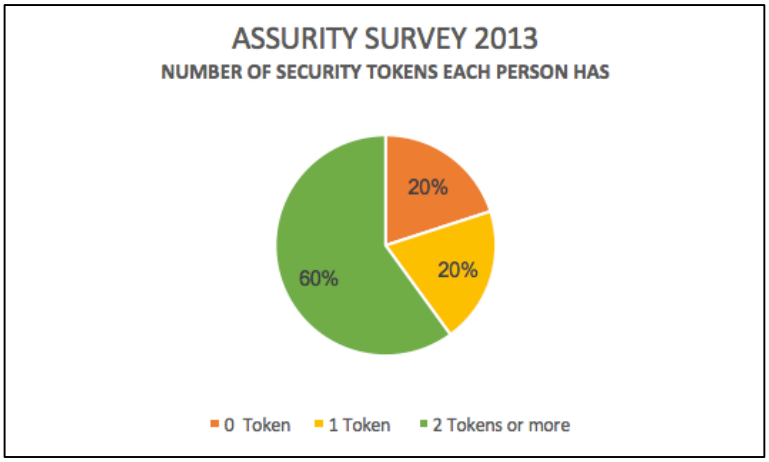

Figure 2.1 Pie chart of number of security tokens each individual has

Assurity (2013) revealed that 60 percent (Figure 2.1) of survey respondents own more than two hard tokens and 43 percent amongst them indicated that their main concern was the inconvenience of having multiple devices which users tend to neglect. iBanking is created on the foundation of providing convenient banking transactions and users are not fully utilizing this service (Appendix Figure B6).

2.3 Recurring replacement and environmental cost

Constant malfunctioning of hard tokens is attributed to the low quality parts used and poor battery life. Statistics have shown that an average of 10 percent of physical tokens (50,000) are replaced per annum amounting to a recurring cost of US$6,500,000 (Securenvoy, 2012).

Banks are casually replacing these tokens are the expense of environmental pollution (Figure 2.2). With the prevalence of environment advocates, the reputation of banks will be negatively impacted for not introducing a solution without compromising on the security.

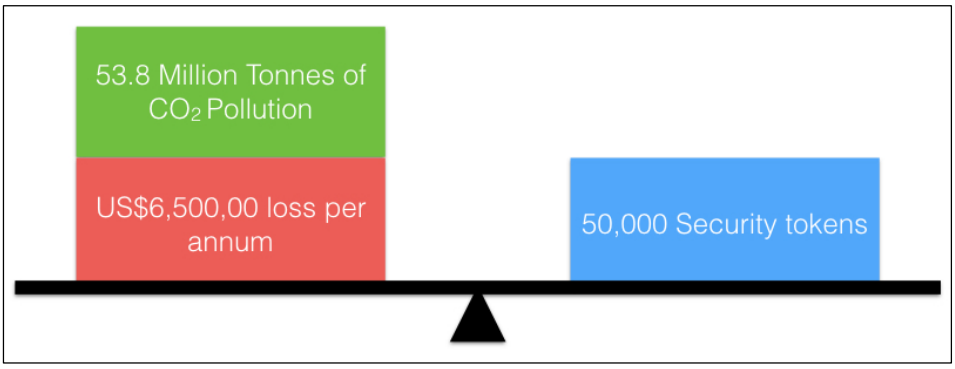

Figure 2.2: Recurring cost of security token replacement

3 MARKET RESEARCH

Primary market research was conducted using a random sampling of 100 Singaporeans to uncover their sentiments on the usability and durability of current 2FA hard tokens and the awareness of the vulnerability of soft tokens.

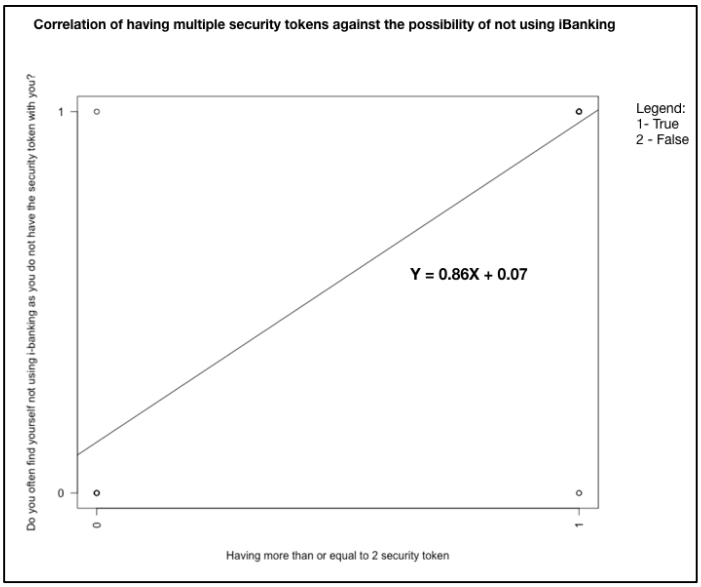

Figure 3.1: Linear regression of response against predictor

Analytical measures from our study drew a high positive correlation[3] of 0.86 (Figure 3.1). Consequently, users with more than 2 tokens are highly likely to underutilize iBanking service as they do not have their hard tokens on-hand. Banks are bearing the repercussion when ease of fund transfer is one of the primary drive to creation of customer value (Goh, Yeo, Lim and Tan, 2015).

[3] Correlation is the statistical measure to indicate the extent to which two variables fluctuate together. A value close to 1 would mean a strong positive correlation, i.e. as one variable increases, the other variable will increase in the same direction, and vice versa.

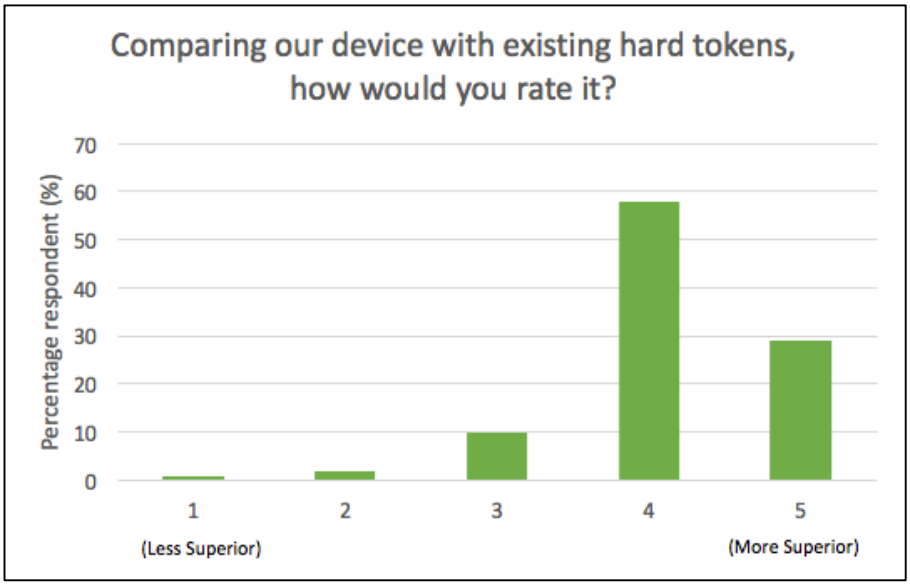

Figure 3.2: Bar graph of rating of Minicure in comparison with existing security tokens

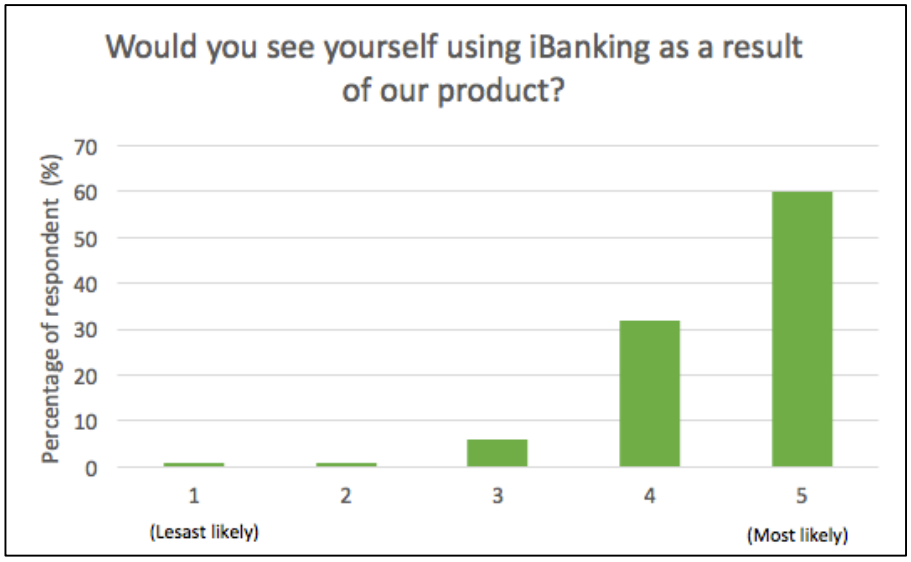

Figure 3.3: Bar graph of increased usage of iBanking as a result of Minicure

87 percent of respondents regarded Minicure to be of higher superiority than existing hard tokens (Figure 3.2). The survey revealed that a high percentage of users (93%) who are not subscribing to iBanking would be intrigued to do so with Minicure (Figure 3.3).

Our primary and secondary research findings are well-aligned to establish the justification for the need of Minicure.

4 MINICURE

Building on the need of an improved 2FA security system and a robust hardware authentication device, we introduce, Minicure (Figures 4.1 & 4.2). Minicure was curated with the aim of striking the right balance between security and convenience.

Figure 4.1: Minicure hardware token

Minicure consists of a physical device complemented with a software application and is developed using proprietary algorithm, equipped with advanced digital signing capability.

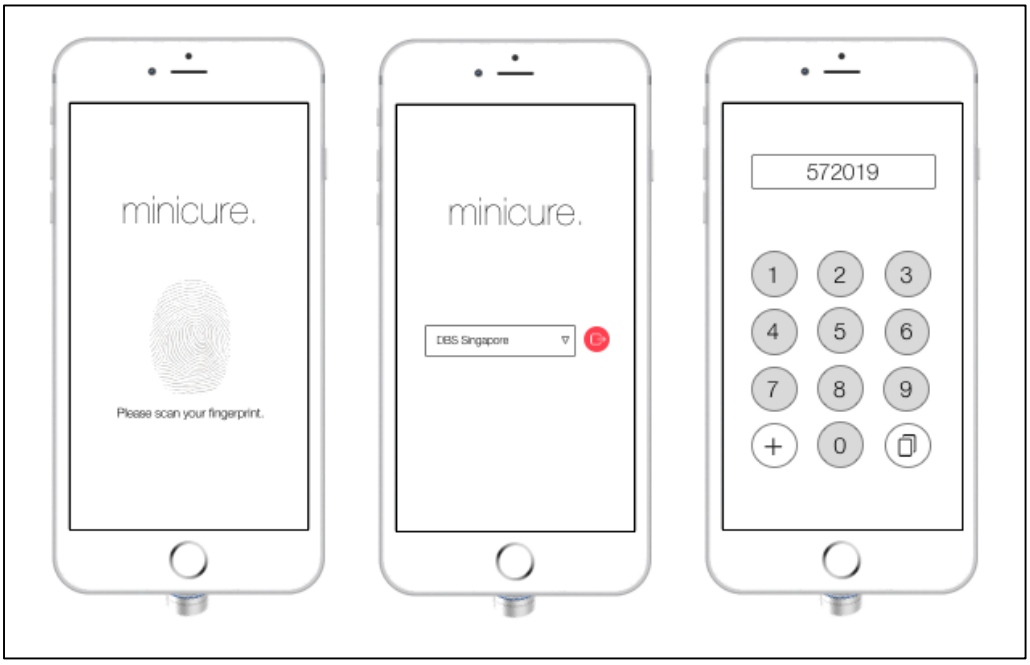

Figure 4.2: Screenshots of Minicure Mobile Application

Minicure functions with the assistance of a mobile device. Upon launching of the mobile application, it will detect for the presence of the token and request for a fingerprint verification. Following which, users will be brought to a familiar interface (Figure 4.2 & Appendix C).

5 BENEFITS

5.1 New Security System

With the prevalent enhanced security features incorporated into today's mobile devices, we would like to challenge ourselves to combine existing technologies on-hand. Henceforth, we tapped on the fingerprint technology to introduce an unparalleled 3FA[4] system whereby verification of the fingerprint is needed to proceed on with using the application.

Our proprietary algorithm introduces an unpredictable dynamic OTP generator which only functions when Minicure is detected on the mobile device. OTP will not be generated upon detection of any malware present.

5.2 Unparalleled Convenience

The mini device is compactable and allow users to perform iBanking transactions on-the-go. Integration of multiple service providers into Minicure will be done in the third phase of implementation (Section 6.1) to address the fundamental issue of owning multiple tokens.

5.3 High Cost-efficiency

We aim to engineer this device withstanding a life cycle of 10 years. High cost efficiency is attained at spreading the one-time cost over the stipulated period.

Minicure tackles the need for annual replacement with the following:

- Powered battery from devices
- Collaboration with Parely[5] - Minicure will be made from recycled ocean plastic furnished with a metallic coating
- IP67[6] verified
- Tracking sensor to prevent loss/theft

[4] 3FA refers to the combination of all of the following authentication factors:

1. The knowledge factor: knowledge of password, pin or pattern.
2. The possession factor: Owning a security token, Automated Teller Machine card or SMS verification code.
3. The inheritance factor: biometrically verified via fingerprint or retina scan.

[5] Parely is a group of environmental activists that aims to raise awareness on the major threats facing our ocean by collaborating with companies on projects to produce items made of ocean plastic. Ocean plastic is made of combination of HDPE (high density polyethylene), LDPE (low density polyethylene) and PP (polypropylene) which are commonly found in ocean trash.

[6] IP67 is the device being totally protected against dust & protected against the effect of immersion between 15cm and 1m.

6 THE DRIVING FORCE

6.1 Product Development Life Cycle

The four-phase implementation is the paramount structure of ensuring the sustainability and scalability of Minicure.

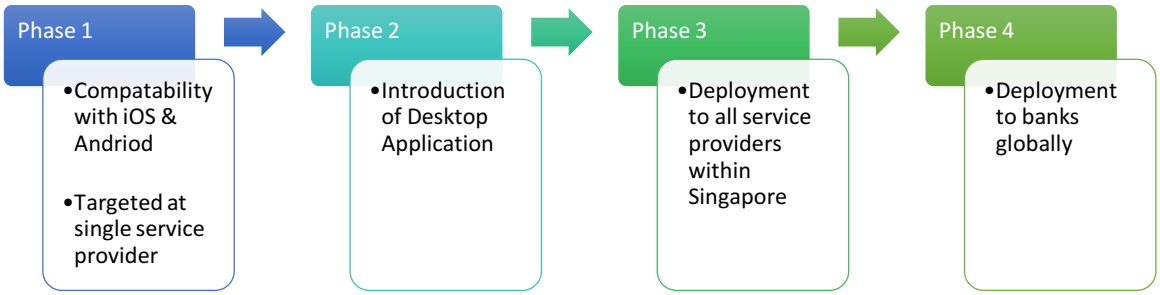

Figure 6.1: Flowchart of Product Development Life Cycle

The second phase will extend our platforms to computers through the connection of universal serial bus (USB) adapters for added level of convenience for users who are constantly on their machines. The subsequent phases involve the partnership of Minicure with all banks within Singapore and eventually, a global launch.

6.2 Target Audience

Minicure's primary target audience will be banks; they will adopt Minicure as the choice of hardware tokens to distribute to their users in place of traditional tokens at no additional charge[7].

[7] Similar to current practice

6.3 Revenue Model

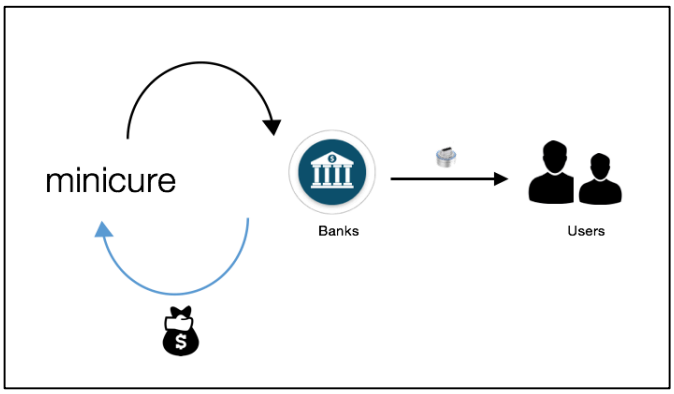

Figure 6.2: Distribution model of Minicure

Minicure is adopting the sales revenue model, projected to generate an operating profit of S$1,300,000 per annum. Banks will purchase the device at a one-time cost. The scalability arises when partnership with banks increases, thereby reducing the cost of production.

6.4 Budget and Use of funding

Description	Amount (S$)
Revenue	
Sales Revenue	10,000,000
Cost of Sale	
Production Cost	2,500,000
Development Cost	5,000,000
Operating Expenses	
Administrative Expenses	200,000
Server hosting	1,000,000
Operating Profit	1,300,000
Return on Investment	14.9%

Your funding will fully support our development costs at building a robust hardware token and a secure OTP server infrastructure.

7 CONCLUSION

Minicure will be the tangible solution to any financial security threats facing 2FA tokens. Minicure will be the low-cost, environmental-friendly and sustainable way of enabling financial transactions on-the-go. Minicure will be the new definition of balance between security and convenience, fundamentally disrupting the internet banking industry.

"The mini device where security lies in you" -- Minic**u**re

TEAM CREDENTIALS

Chua Kim Hong, Ashley (Ms.)
B.Sc. in Computer Science with Minor in Information Security
Chief Technology Officer
Square Inc.

Tan Qing Yang (Mr.)
B.E. in Materials Science and B.A. in Business Analytics
Chief Engineer
Square Inc.

REFERENCES

assurity: Trusted Solutions - Newsroom - Press Releases. (2013). Assurity.sg. Retrieved from http://www.assurity.sg/news_press.html

Baker, S., Filipiak, N., & Timlin, K. (n.d.). *In the Dark: Crucial Industries Confront Cyberattacks* (1st ed.). McAfee. Retrieved from http://www.mcafee.com/sg/resources/reports/rp-critical-infrastructure-protection.pdf

Goh, M., Yeo, S., Lim, K., & Tan, S. (2015). *Understanding Customer Satisfaction of Internet Banking: A Case Study In Malacca* (1st ed.). Malaysia: Multimedia University, Melaka. Retrieved from http://ac.els-cdn.com/S221256711630096X/1-s2.0-S221256711630096X-main.pdf?_tid=fad1f598-9117-11e6-ad20-00000aacb360&acdnat=1476344466_8d7a95420f2fa3c13c6148e91aa48abc

Hummer, L. (2016). What's Wrong with SMS Authentication? Security Intelligence. Retrieved from https://securityintelligence.com/whats-wrong-with-sms-authentication-two-ibm-experts-weigh-in-on-the-nist-recommendation/

Wueest, C. (2016) (1st ed.). Symantec. Retrieved from http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/financial-threats-2015.pdf

You can’t put a price on security, yet Security can Literally Cost the Earth – SecurEnvoy Blog. (2012). SecurEnvoy Blog. Retrieved from https://www.securenvoy.com/blog/2012/02/02/you-cant-put-a-price-on-security-yet-security-can-literally-cost-the-earth/

Appendix A: Primary Research - Survey Questions on Internet Banking

Internet Banking - Security Tokens

This survey seeks to uncover the functionality and usability of security tokens used in internet banking and user's awareness of the vulnerability of soft token (SMS OTP) verification for Two Factor Authentication (2FA).

* Required

Do you use Internet Banking? *

- ○ Yes
- ○ No

How many banks do you have an account with? *

- ○ 1
- ○ 2
- ○ 3
- ○ Other :

How many security tokens do you have? *

- ○ 1
- ○ 2
- ○ 3
- ○ Other :

How often do you replace your security token? *

- ○ Once a year
- ○ Once every 6 months
- ○ Once every 3 months
- ○ Every month
- ○ Never
- ○ Other :

If you have replaced your security token before, what is the reason for the change?

- [ ] Battery issues
- [ ] Faulty buttons
- [ ] Product Malfunction

Do you often find yourself not using i-banking as you do not have the security token with you? *

- ◯ Yes
- ◯ No

Are you aware that SMS OTP is more vulnerable to security (malware) attacks as compared to using the security token? *

- ◯ Yes
- ◯ No

This is our product.

Maximum protection from malware | Able to generate an OTP with any banks in just one device | Small & convenient

Comparing our device with existing hard tokens, how well would you rate it? *

	1	2	3	4	5	
More inferior	◯	◯	◯	◯	◯	More superior

Would you see yourself using iBanking as a result of our product? *

	1	2	3	4	5	
Least likely	◯	◯	◯	◯	◯	Most likely

Appendix B: Primary Research - Respondents

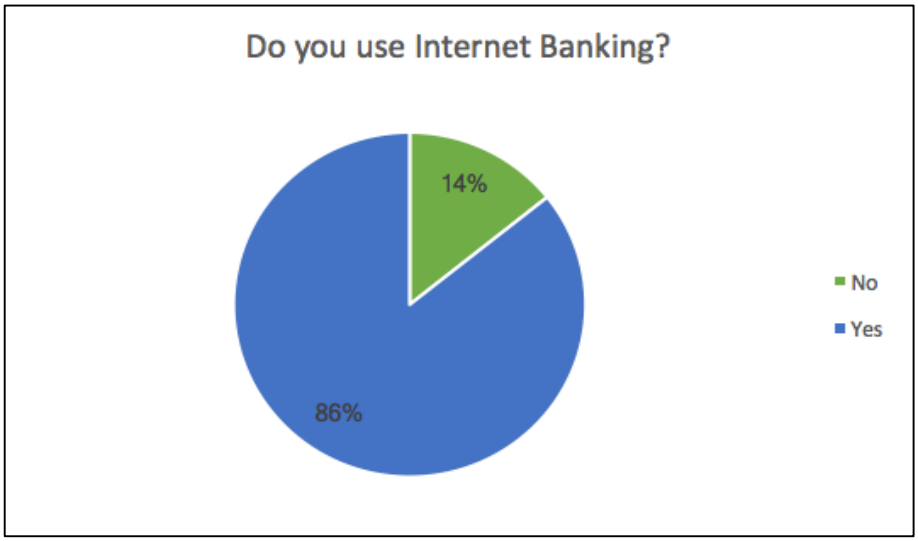

Figure B1

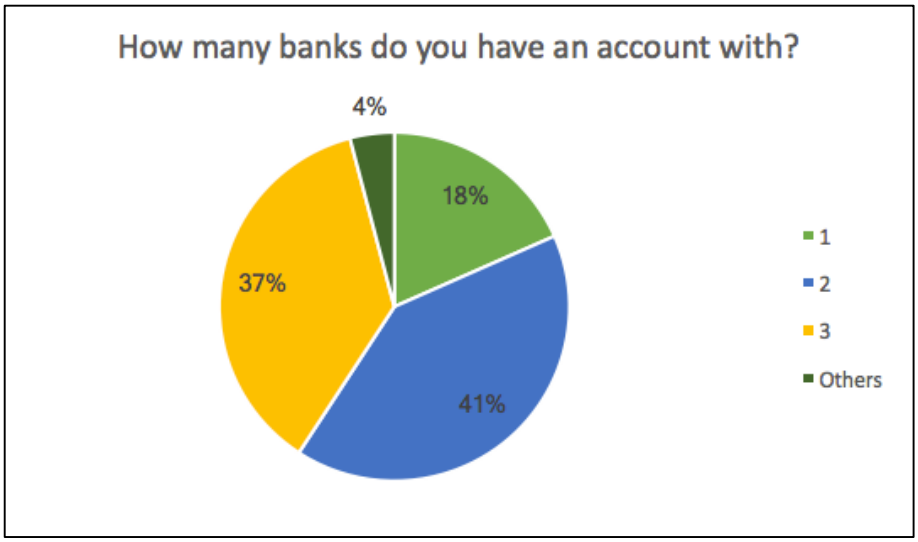

Figure B2

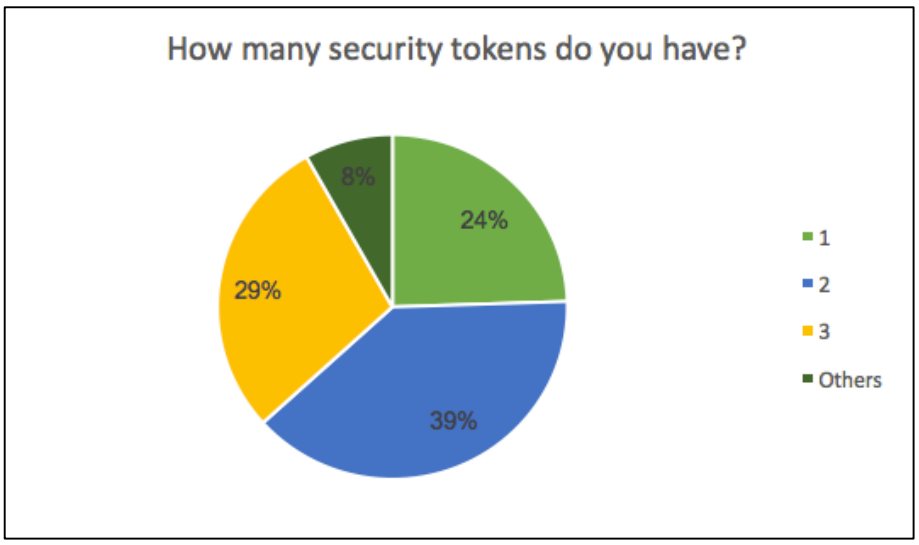

Figure B3

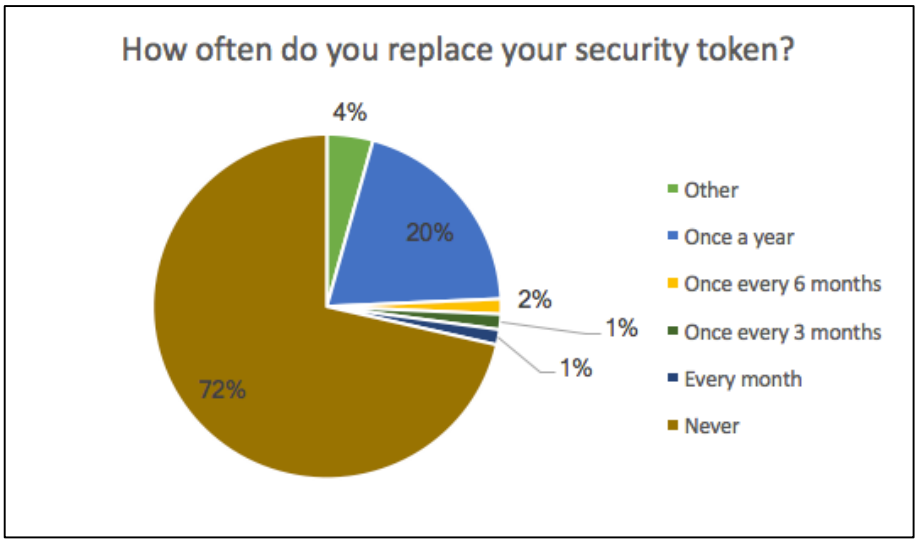

Figure B4

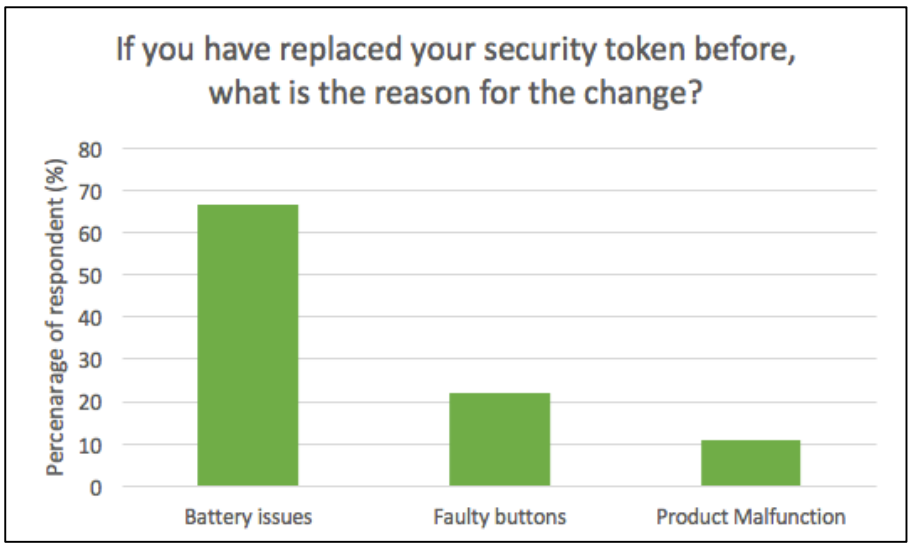

Figure B5

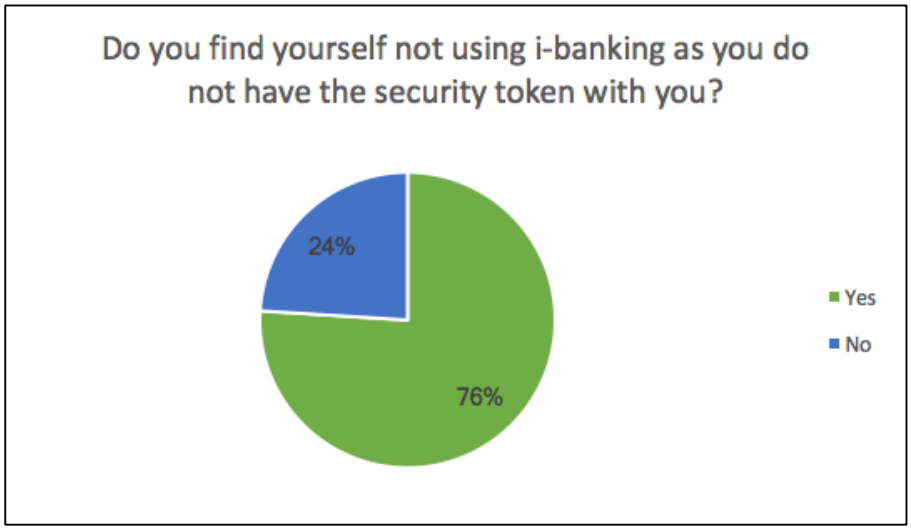

Figure B6

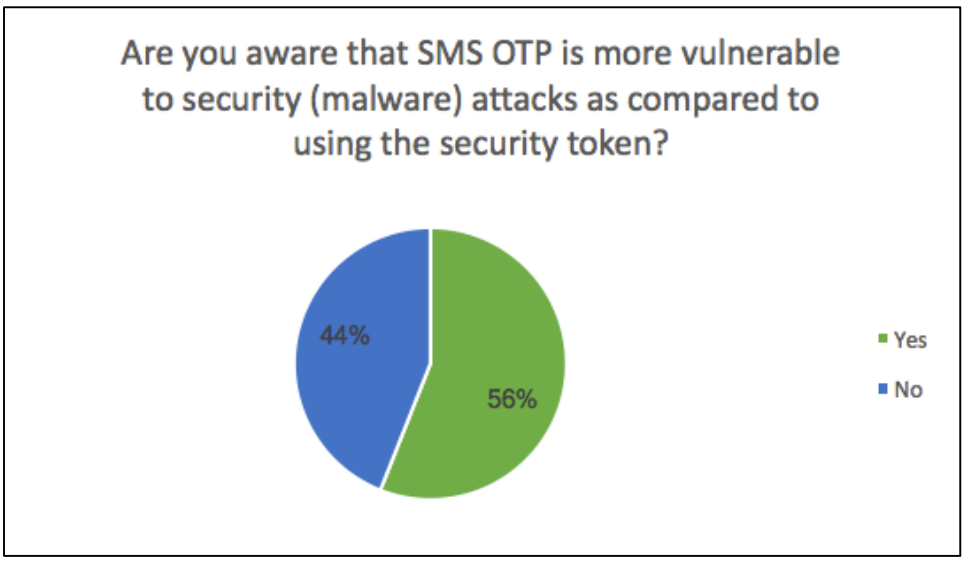

Figure B7

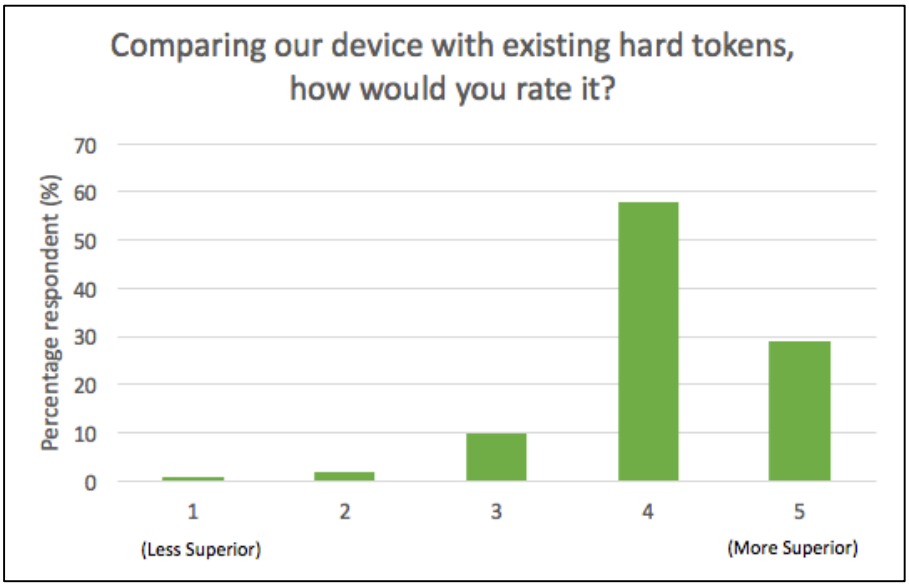

Figure B8

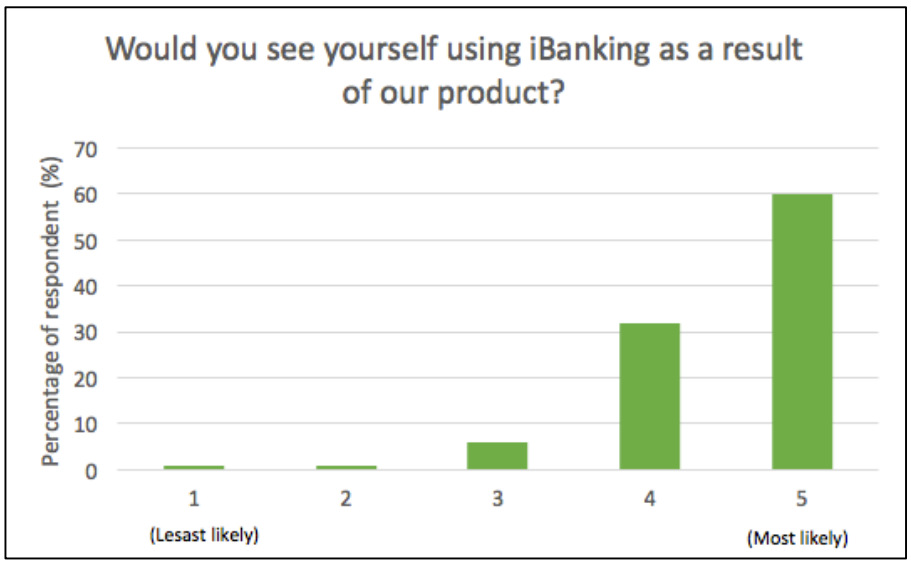
Would you see yourself using iBanking as a result of our product?
Percentage of respondent (%)
70
60
50
40
30
20
10
0
1
2
3
4
5
(Lesast likely)
(Most likely)

Figure B9

Appendix C: Minicure

Minicure will be available on major mobile application stores.

Figure C1: Mobile application screenshot of landing page if device is not connected

Upon the launch of the mobile application, users will be prompted to insert the token device.

Figure C2: Mobile application screenshot of fingerprint verification page

Upon insertion of the device, users will be prompted to verify their fingerprint using the mobile devices' fingerprint sensor.

In an event where Minicure is 15 meters away from your mobile phone, a notification will sound off to alert the user that he/she has left his/her Minicure behind. Users will have the option of switching the tracking sensor off.

Figure C3: Mobile application screenshot of bank selection

Following which, they will be prompted to select the desired banks that they wish to perform the transaction with.

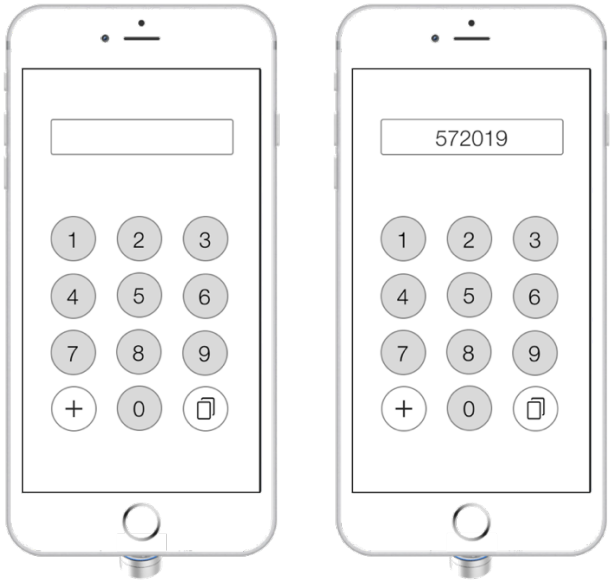

Figure C4: Mobile application screenshot of token interface

An additional feature introduced would be the ‘copy to clipboard’ function which aims to enhance the usability of Minicure. Users need not put their memory to test when inputting the OTP into banking applications or websites running on the same mobile device.

Upon selection of the chosen bank, users will be brought to an interface similar to the traditional hardware token. Users can either select ‘+’ to generate a new OTP code or the ‘copy’ icon to copy the OTP to their clipboard. The OTP will be valid for a mere 60 seconds.

Appendix D: Square Inc. - Company Profile

Square

Square Inc., a San Francisco based company, offers financial, merchant and mobile wallet services. It specializes in marketing payment programs based on their Square Reader device. Jack Dorsey and Jim McKelvey founded the company in 2009, launching the company's services and app the following year. In November 2015, Square began trading on the NYSE. Square now has a market value of $3.2 billion.

Square Inc. is currently looking at expanding its businesses to extend the products and services offered by establishing a production factory. Minicure will be the enabling project for this expansion.

Square Inc.
36 Armenian Street
#02-02
Singapore 179934
(T) 6823 2320