THE UNIVERSITY OF HULL

Authorising M-commerce with location

being a Thesis submitted for the Degree of Master of Science in Digital Media

in the University of Hull

by

Jason Hayhurst, BSc (Hons)

September, 2014

Acknowledgements

I would like to thank my personal supervisor Dr Darren Mundy for his continual support through my research. The supervision received has provided the guidance needed to keep me on the correct path to complete the research.

I would also like to thank the survey respondents that took the time to complete the questionnaire.

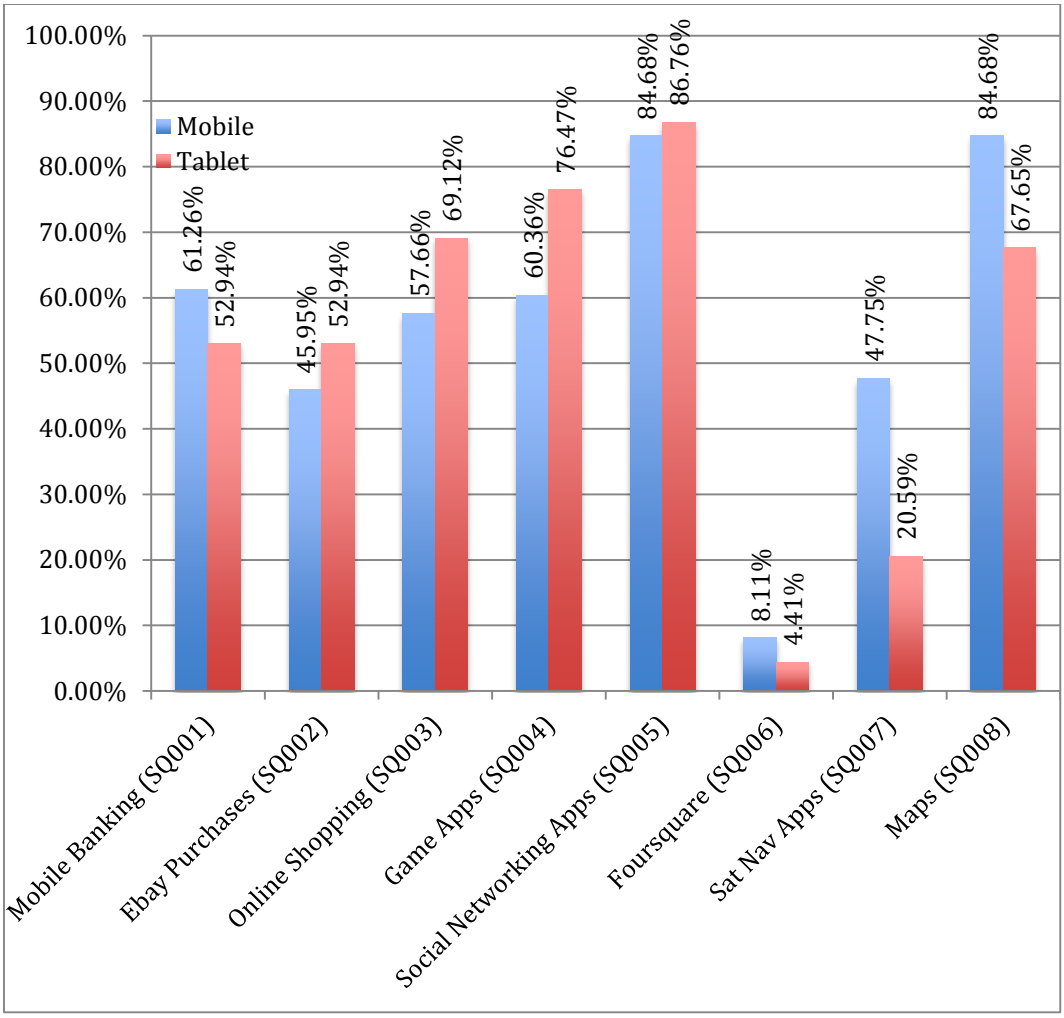
Abstract

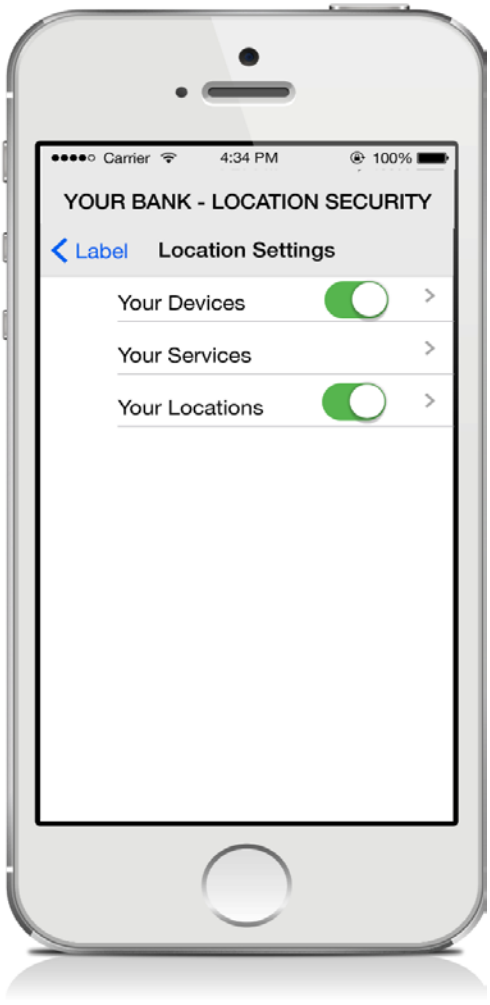
Global fraud in 'cardholder not present' transactions over the World Wide Web continues to grow, in line with the ever-increasing numbers of transactions carried out over this medium. Unfortunately, at present the measures designed to combat against this fraud continue to require improvements to be made to limit the fraud. In this paper we will propose a series of indicators that financial service providers should consider in their attempts to limit fraudulent transactions. The indicators make use of prevalent technologies coupled with a need to place more power to limit fraud in the hands of the customer, especially given banks are continually moving responsibility onto the customer to protect their data.

Whilst the banking sector uses a variety of measures for fraud detection at present there is only limited usage of device related indicators that customers could establish to limit the fraud on their account. For instance, whilst many users will have multiple devices the likelihood of a user performing a valued transaction on a device outside of that subset of devices is limited. Therefore, an indicator linked to device usage controlled by the customer may help to introduce further difficulties for the individual attempting to commit fraud. Similar indicators exist linked to device geo-location, service usage, time determinants and other aspects.

This thesis demonstrates that users do not find device location services too complex to use. Indeed, providing user controls to enabled personalised security settings increase users trust levels. This research proposes security controls are embedded within users banking application. The effect of this approach increases users willingness to engage with location based security controls. Any initial privacy concerns are overcome as long as the proposed controls remain within the banking application.

Table of Contents





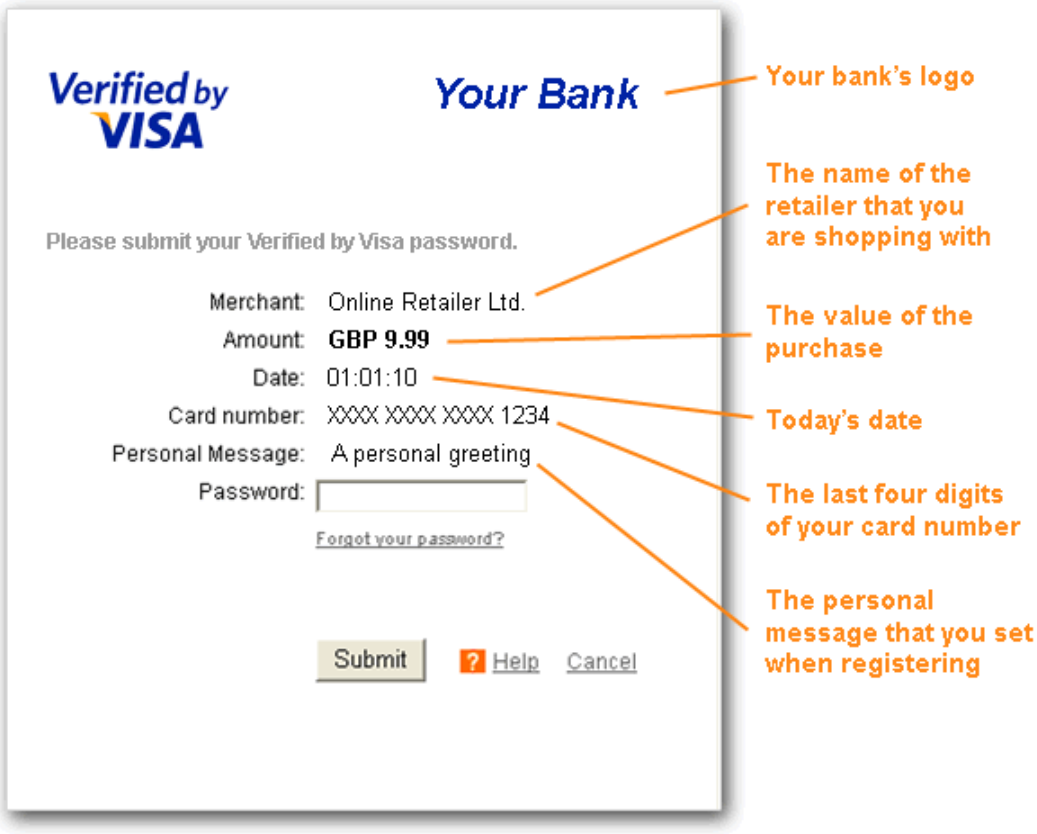


Table of Figures

Table of Tables

Chapter 1 Introduction

1.1 Background & Motivations

Ecommerce now forms a substantial part of the global commerce infrastructure, with individuals increasingly purchasing items over web-based channels as opposed to more traditional face-to-face or telecommunications type purchases. Unfortunately, as with any environment in which substantial amounts of money are involved, criminals are targeting ecommerce environments in order to de-fraud the consumer. According to World Pay (a significant global financial institution providing ePayment solutions for the web) at present up to 42% of customers (in a sample of 19000) who do business online have experienced fraud or are aware of fraud that has occurred to a close friend or family member (Worldpay, 2012). This percentage is very high, and demonstrates the significant risk now involved in web based ecommerce processes.

In the UK the costs of fraud for online purchases cost £163 million in 2013. Furthermore, 23% of people in the UK have received a cold call requesting personal or financial information. 39% said that they found it difficult to tell the difference between genuine and fraudulent calls (Financial Fraud Action UK, 2014). Online purchases do not benefit from physical purchase protections like Chip and Pin.

Many online banks have encouraged retailers to implement a system called 3-D-Secure which requires customers to enter a password before allowing the transaction to be authorised. Some banks, however, such as the Royal Bank of Scotland have since made changes to their customer terms and conditions to what they refer to as RBS Secure. The clause states that “You understand that you are financially responsible for all uses of RBS Secure” (Royal Bank of Scotland, 2015). The problem with the change in banking terms and conditions is that customers can be now considered liable for fraud. The UK Cards Association (UKCA) only record losses of the banks and merchants but they do not monitor customer direct losses when the banks consider them liable for a claim. In the first half of 2012 the Financial Services Authority reported 483,666 complaints against disputed charges and it could be argued that there

is therefore an additional unreported amount of fraud that banks have disputed and past onto the consumer themselves (Murdoch, 2013). Fraud from online purchases could therefore be significantly higher than the data reported by the UKCA. This change in banking terms increases customers' financial responsibility as a result from fraud from online purchases.

There has also been media coverage of cases whereby customers have experienced card fraud and the bank has disputed the claim. One example was when one person was sent a replacement card to his UK home whilst working in Bangalore. He claimed the card never arrived but someone else started using his card in Mumbai running up a bill of £3000. The bank claimed the cardholder was involved in the fraud but after involving the financial ombudsman they only paid out the claim as a matter of goodwill (Brignall, 2012). Additional cases in the article demonstrate banks refusal to pay claims when they consider the customer to have been negligent in the care of their PIN data. In cases were people have written down PIN numbers in wallets and then had them stolen the banks consider a breach of terms and conditions. As the burden of financial responsibility shifts more towards the consumer there is the need to consider additional lines of security or defence so that when one is breached another can act to limit the financial exposure to the consumer.

The penetration of mobile devices in nations worldwide continues to increase with mobile subscribers estimated to total 6 billion in 2012 (mobiThinking, 2013). According to "Mobile Commerce – From Evolution to Revolution" (Roman and Bergholtz, C, 2012) the M-Commerce market is expected to grow by 47% over the period 2011-2015 with this equating to 9% of the ecommerce market globally. This 9% will not be evenly spread across nations. In some nations M-Commerce will become the main method of ecommerce given the quality and size of the mobile telecommunications network as opposed to the physical network infrastructure. One of the major issues in this growth is security with users facing issues with respect to trust on mobile platforms. These trust barriers are in some respects greater than for existing methods of

ecommerce as the M-Commerce platforms are newer and can be unfamiliar to users.

One advantage of smart phone devices is the built in capability of using GPS to provide location to a range of applications. The Global Positioning System (GPS) is a U.S.-owned utility that provides users with positioning and navigation (U.S. Goverment, 2013). The satellites orbital positions are evenly distributed so that no matter where you are on the planet you should be able to access at least 4 of the satellites in order to calculate your position (*Ibid*.,p5-7). The accuracy of positioning data on smart phone devices has been enhanced with the introduction of wireless fingerprinting (Zandbergen, 2009). This is where a number of wireless positioning systems use a collaboration phase to position a device with a greater accuracy than GPS alone. Public databases exist of current wireless access points and their GPS co-ordinates. Many devices now use this database to calculate more accurate positioning of devices even within an indoor location. The Apple iPhone makes use of the "Skyhook wireless" database of public access points to provide positioning of the device (Skyhook Wireless, 2011). The positional technologies described above enable context-aware services to make use of a smart phones device location in order to engage with the user more relevantly. Foursquare and Facebook both allow check in facilities with smart phone devices to share the users location. There are also many GPS Sat Nav applications that use positioning context from a smart phone device, however, at present there does not appear to be smart phone applications that use location to restrict where they wish to use different services.

M-Commerce covers a range of different devices including everything from a user's mobile device through to tablet computers, but essentially focuses on transactions made whilst moving around locations, through devices which move with the user. Users often will use a variety of different devices to make their purchases, in some cases they will use only specific devices to carry out some transactions (often because of issues related to the interface), in other cases users will use all of their devices to carry out their business just in

different places. For example, John may have a mobile phone, tablet and his work PC. John may use his work PC to only purchase items from particular vendors linked to his work, whilst he may use his mobile phone to carry out transactions with particular eBusinesses and use his tablet to access eBanking services. At present though the way in which a user utilises their devices and the linkage between a user and their device does not form part of any fraud detection process.

Authentication is the process of individual parties proving they are who they say they are to other individuals or businesses. On the web generally organisations authenticate to users through the use of a secure protocol called Secure Sockets Layer (SSL), in this protocol businesses provide digital credentials (in the form of x509 certificates) to users and these credentials are checked by user systems (e.g. the web browser) to ensure that the business is who they say they are. On the user side, in general, authentication comes through a process of a user providing some form of identifier to the eBusiness organization to prove their identity. In a substantial number of cases this identity check is carried out through the use of a username and password. Often these identifiers are the targets of criminals with the use of various technologies (e.g. a key logger or similar) or social engineering processes designed to capture these from users. Therefore the process of user authentication apart from in eBanking scenarios is generally inadequate to protect users and businesses against fraud on the web.

Authorisation takes place after a user has authenticated and it is the security mechanism that decides what functions a user can or cannot carry out. Within the context of smart-phones it is the level of access within a mobile application or service that the user has permission to use. When a password is compromised then criminals have no further barriers to using the services other than the level of access granted to the user.

The intention of this MSc project is to examine the link between a user and their devices, such that device locations are included in the authorisation and fraud detection process. The process of registering devices and stipulating

what these can be used to do is not particularly new. Major retailers whose business is formed around limiting user access across multiple devices already provide these services. For example, film-streaming providers such as Netflix, iTunes and Sky Broadcasting limit the amount of concurrent devices per account in order to provide some control of customer usage and account sharing. However, there is at present no direct linkage between these services and M-Commerce.

Using location as a means of authentication is not without risk. GPS receivers are vulnerable to attacks such as blocking, jamming and spoofing. These attacks work on the basis of denying or modifying the location reported but often lead to loss of signal in the GPS receiver. Presently there are no implemented countermeasures for GPS spoofing. The military GPS signal is encrypted but the civilian technology is not (Wen et al., 2005). There has been research into monitoring signal strength to aid spoof detection but this is not a protection system rather a form of intrusion detection.

The use of GeoEncryption keys has been researched in order to use location as an additional authentication factor for smart phone mobile applications (Kuseler and Kami, I A, 2012). This research introduces an expected receiver's location as an encryption key. The actual location is then used as a decryption key and only unlocks the message if the user location is within a tolerance-based location of the expected location. The challenge with this approach is consideration of the user's privacy. The paper suggests that it may be possible to use privacy-preserving algorithms to solve concerns. Implementing encryption methods suggested in the paper are still prone to attacks. The location needs to be independently verified so that an attacker cannot claim to be in the location. More research is required into the GPS receivers in smart phones as these can also be manipulated using proxy servers unless the location is verified using cell towers.

The use of device registration services for private and public network domains has already been recognised as a mechanism for introducing more substantial security to wired and wireless networks. For example, the Devices Profile for

Web Services (DPWS) system (Oasis, 2009) has recently been introduced to help to enable device registration within home and office environments. DPWS provides a mechanism to provide Public Key Infrastructure (PKI) services within a network environment that can help to protect the network through the use of device authentication services. One of the main issues with such services has been in the past concerns over their ease of use.

Muller et al. (2010, pp.118-122) and Lee et al. (2008, pp.33-48) have proposed a device authentication system for home networks that enables users to provide digital certificates to authorised devices. This system means that if a user connects to a home network without a digital certificate they will be limited in what actions they can perform through that network system. In addition, device authentication systems built on PKI services have been introduced by Sanchez-Guerrero et al. (2011, pp.1-5) in the context of WiMax networks providing device authentication and authorisation through the use of device based Identity Cards and the Security Assertion Mark-up Language (SAML). Users' profiles and device profiles are constructed for individuals who have authorised access to the network. These profiles work in conjunction to provide assurance within the network that an individual user using a particular device is authorised to be present in the network, and to perform any actions requested. However, these solutions have not been looked at in the context of global ecommerce and any solution required for global ecommerce is likely to need to be much more scalable than the above state of the art designs.

There are numerous services that could make use of location as an additional means of authentication. Banking services including VISA and MasterCard could use this to further reduce fraud for their customers. This could form part of mobile transactions taking place similar to 3D secure verification process. At the stage a customer wishes to purchase something on their smartphone the location could be checked against an acceptable pre agreed location. The banking sector could also use it to prevent unauthorised access to online banking from mobile devices. The music and film industry could also benefit from this approach. For example, Netflix, Sky, Lovefilm restrict the number of

concurrent streams based on the device registered. It may be of interest to them to restrict access by location to avoid people sharing account login information with friends or families.

1.2 The Problem

Section 1.1 describes a significant amount of fraud taking place on an annual basis in the “cardholder not present transactions” most commonly found on the World Wide Web. Much of this fraud is brought about through poor user security practices, simple attack mechanisms, and flaws in current financial transaction processes. For example:

- Users are notoriously poor at choosing good passwords and at password management, this causes problems as for many systems at present the user authentication process uses password-based solutions;

- More secure security infrastructure such as PKI is not used ostensibly in controlling authentication and authorisation processes;

- Financial services themselves still do not in general provide mechanisms to securely identify themselves to the user (other than general browser based mechanisms).

- Locking down groupings of mobile commerce transactions is not presently considered.

With the amount of money spent online continuing to increase there exists a need to look at ways in which this fraud can be further limited. In this regard it is useful to consider that current mechanisms that users use to facilitate their business transactions on the web, are not currently viewed as part of the authentication process. Therefore this research intends to examine whether viewing such devices as part of the identity management process can help to facilitate further restrictive practices on the use of the devices themselves, for example, restricting the use of such devices in location based scenarios. In particular the research will consider whether users will accept this additional layer of security or not.

1.3 Aims and Objectives

The aim of this research is to investigate to what extent typical smartphone users are willing to use their device location as a method of reducing their exposure to mobile commerce fraud attempts and what services the users would want to restrict.

1.3.1 Research Question

How can location-aware technologies be used in financial environments to reduce users' exposure to fraud?

Are users willing to consider the use of location-aware technologies linked to financial services as a mechanism for reducing fraud?

What are the challenges involved in linking location-aware services to realise a solution, which meets user needs whilst providing an extra layer of security for financial transactions?

1.3.2 Objectives

The objectives of this research are as follows:-

- Provide a thorough review of how location is determined on a smartphone and the enabling technologies. Identify the challenges in determining location.
- Investigate the state of the art using smartphone location as a means to authorise mobile services.
- Identify any current limitations and issues with using location as a means of authorisation.
- Design and develop a user study to investigate user willingness to use location to authorise mobile services.
- Analyse the study of users to form a basis for the development of a conceptual idea(s).

1.4 Methods of Research

This section details the methodology and the background to the justifications for the approaches taken in order to conduct effective research within this thesis.

1.4.1 Study Background

Ofcom state that in 2014 six in ten UK adults use a smartphone which is an increase of 54% since 2012. The age ranges that have driven this increase is by 25-34s and 45-54s, and those aged 65-74 are almost twice as likely to use a smartphone now compared to 2012 (20% vs. 12%) Furthermore the report shows that online transactions are also popular; two in three (66%) internet users make online purchases and six in ten (61%) do online banking or pay bills online at least quarterly (Ofcom, 2014). This significant smartphone usage in the UK inconjunction with high usage of online banking services make the UK a suitable country to survey relating to this study

1.4.2 Survey Population

The survey population in this research are based the UK. An initial survey was used to identify users that use online banking services via a smartphone. Participation in the survey was voluntary and conducted anonymously online.

1.4.3 Methodology and Measurement Approach

The research in this thesis is formulated using empirical research methodologies. The surveys designed will enable quantitative and qualitative data to be collated and analysed.

In order to test users willingness to engage with location-based mobile security, a survey instrument has been developed after reviewing user acceptance frameworks in chapter 3. The surveys created use a five point unit of measurement on the Likert scale. The scale will range from strongly disagree to strongly agree.

1.4.4 Survey Data Collection Method

The survey data was collated using the open source survey tool called Lime Survey. Two surveys were created in this research. Prior to the initial survey a pilot survey was carried out with a smaller population sample. The results of the pilot surveys are shown in section 3.3.3 of this thesis.

1.4.5 Research Process

The following methods will be used to address the objectives defined in section 1.3: -

Undertake a written review of location enabling technologies. The information from this review will be written in section 2 of this report. This section will be split into location technologies, access control lists, challenges in determining location on smartphones and a review of using location as a security factor.

An online survey will be designed and after ethics clearance has been approved for this project the survey will be deployed online to over 100 candidates. The results will then be analysed and presented in this report.

A case study will be created from a subset of the people surveyed. The results of the survey will be analysed and presented in this report.

The information from the survey and literature review will be used to design workflows of a basic prototype application.

An appropriate focus group from the initial survey respondents will be selected to test the effectiveness and ease of use of the basic prototype application. Questionnaires and observations will be carried out and the results will be concluded in the report.

A conceptual framework will be included in this report to outline how the location authorisation could be implemented.

1.5 Organisation of Report

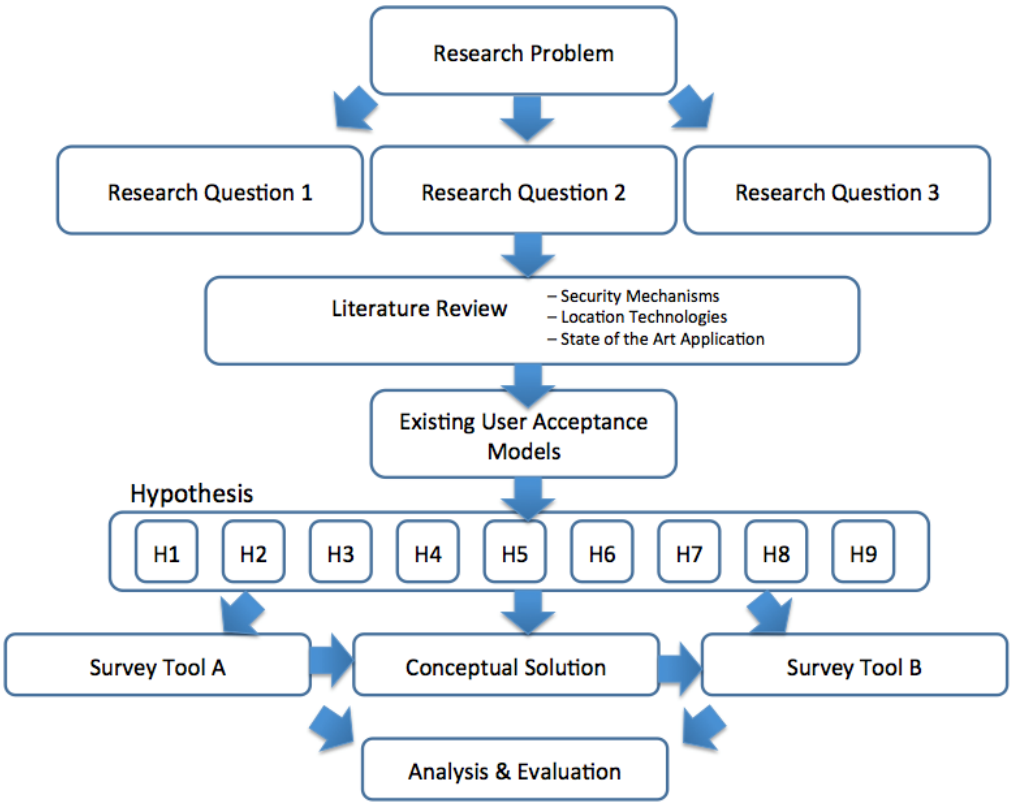


Figure 1. Structure of Dissertation

Figure 1 is a visual representation of the structure of this research. The introduction of this report (Chapter 1) outlines the growth of M-commerce transaction and mobile devices. It highlights differences between authentication and authorisation with justification of the problems that still exist in not using location-based services as a form of fraud protection. This chapter also presents the aims and objectives of this research towards the design of an example application that can be used to test user willingness to engage with location-based authorisation on mobile devices.

The literature review (Chapter 2) details research of available technologies, state of the art and challenges with location-based services. Chapter 3 reviews user acceptance frameworks in order to be used as a foundation for the survey in chapter 4 of this research.

Chapter 4 shows the development, testing and results of the initial survey about users' device habits and their opinions and use of location-aware

services. The results of this survey were then used to influence the design of a proposed location-aware authorisation application as part of a user's mobile banking application. The design of the application is shown in chapter 5. The design of the second survey is also in this chapter, which was given to a smaller focus group from the original survey.

Chapter 6 shows the results and analysis of the second survey after the users had seen how the example application worked.

Chapter 7 details the analysis of both the surveys with any significant findings. There is then a conclusion in chapter 8, which evaluates how well the project has met the objectives stated in section 1.3.1 of this report. In addition, at the end of the dissertation further work is detailed.

Chapter 2. Review of technologies and the state of the art in delivering location services.

2.1 Introduction

This chapter reviews how location is determined on a smartphone device and the challenges in determining location. Authorisation and authentication based services are reviewed in relation to using location as a security factor. Any current limitations and issues will be summarised at the end of this chapter.

2.2 Context-Aware

Managing contextual information in a mobile environment can be complex, as it is by its nature dynamic (Zhang et al., 2009). This can be due to the data coming from different sources such as location, user ID or mobile number. Zhang (*ibid)* presents a useful framework to help conceptualise a detailed version of the main components of context-aware mobile systems. These are made up of: -

Physical – This is the technology layer to identify the location of the user e.g. GPS, A-GPS.

Virtual– This layer is related to contextual information on a smartphone such as calendar and appointments. This could also be an app installed on the smartphone.

Logical – This layer is a combination of the two proceeding layers to deliver context. For example, the use of the current location (Physical Layer) in conjunction with a banking application on the device (Virtual) that queries an online database for that user to decide if the service has been authorised to access from the current location (Logical).

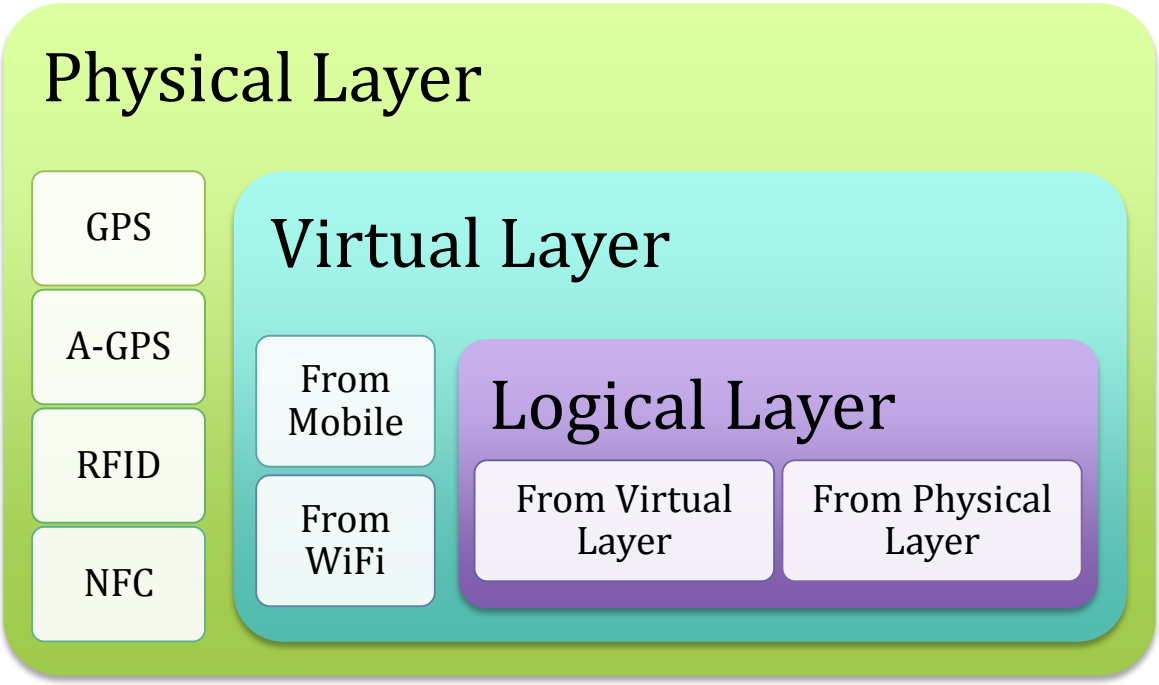


Figure 2. Representation of context-aware layers

Figure 2 forms part of the framework for this research and is an aid to conceptualise the model for context-aware systems. This concept shows there is a need to store data from these levels in order to make sense of the combined data-set to provide context-aware information to the smart-phone.

2.3 Technologies that enable location-aware services

There are ranges of technologies that enable location-aware services detailed in this section. It should be noted that a smart-phone will attempt a combination of the location technologies that are available in order to provide the most accurate positioning. In some instances that may include triangulating the position using the signal strength from the nearest mobile masts.

2.3.1 GPS

The Global Positioning System (GPS) is a U.S.-owned utility that provides users with positioning and navigation (U.S. Goverment, 2013). Section 1.1 provides an overview of how the GPS network provides signalling. Each satellite broadcasts its location, status and precise time using atomic clocks. A GPS device receives this data and calculates its distance from the satellite using the formula (distance = rate x time) where rate is the speed of light the

signal travels from the satellite to the GPS receiver. Time is how long the signal travelled through space, which is calculated by deducting the arrival time on the GPS receiver from the transmitted time stamp from the satellite. When the receiver has completed the calculations from at least 4 of the 24 orbiting satellites it has sufficient data to provide 3D telemetry. According to the US Government the worse case scenario accuracy of positioning is 7.8 metres (*ibid).*

2.3.2 A-GPS

GPS was originally intended to be used outside where a GPS receiver had clear view of satellite signals. Today, GPS is also expected to work inside buildings. Some applications require a relatively fast fix on the current position. To aid this process assisted GPS (or A-GPS) was created. A-GPS uses location servers that keep a constant list of satellite positions and in turn feed this information to GPS receivers via cell towers. This results in a faster first fix on position that would otherwise be potentially difficult to achieve indoors (Van Diggelen, 2009).

2.3.3 Wireless fingerprinting

Many offices and public locations now have wireless access points. Many of these access points may have a level of security applied to prevent unauthorised access to the wireless networks such as WEP or WPA security protocols. The rise of ubiquitous access points makes using them for positioning very cost effective as it minimises any additional hardware infrastructure required.

There are a number of wireless positioning systems that use a collaboration phase to position a device. This is known as wireless fingerprinting (Zandbergen, 2009). Public databases exist of current wireless access points and their GPS co-ordinates. Many devices now use this database to calculate more accurate positioning of devices even within an indoor location. The Apple iPhone makes use of the “Skyhook wireless” database of public access points to provide positioning of the device (Zandbergen, 2009), (Skyhook Wireless, 2011).

Technology	Features
GPS	• 24 orbiting satellites provide positioning info to GPS receivers. • Good for outdoors positioning. • Not good for indoor positioning.
A-GPS	• GPS data stored in location servers. • GPS receiver's hardware can be lower spec and save battery power. • Faster positioning results.
Wi-Fi Positioning	• Ubiquitous Wireless Access points can be used to provide positioning information to smart-phones. • Global databases of access point used to provide positioning when GPS, A-GPS not available. • Cost effective in an educational environment, as access points already exist in many institutions.

Table 1. Summary of Technologies that enable location-aware services

2.3 Access Control

Access control is a means of constraining what a user can do and also what programs running on behalf of a user can do (Sandhu and Samarati, Pierangela, 1994). There are a number of different access control methods which will be detailed in this section.

Authentication is the process of checking a user's identity. Verification can include checking a password, a biometric signature such as fingerprint or a retina scan. A security system checks the data provided against its records before allowing access. Once approval has been received the user is effectively authenticated. Authorisation usually works in conjunction with authentication by taking a record for an authenticated user and deciding what resources they are authorised to access. An example of authentication and authorisation is provided through Microsoft Active Directory. Active Directory is the security database for domain controllers in a network. When a user logs

onto a pc they have to enter their user id along with a password. The details are verified with the records held in active directory and if correct they are allowed to login to the network (authentication). When they open a network share to access a document on a file server, then active directory checks the permissions set for that user or their group and applies them (authorisation). In this example the user may have read, write or modify permissions to that file.

Figure 3 is an details the process of accessing a document or resource from authentication through to authorisation based on the access control and other security services diagram in the Access Contol: Principles and Practice journal (Sandhu and Samarati, Pierangela, 1994, p.41). Once a user authenticates the reference monitor checks whether the user has sufficient privileges to access the resource or document from the authorisation database. Access attempts are usually logged in a separate database for reporting purpose.

The problem with this traditional access control model is the single point of failure. A hacker only needs to discover the password data in order to gain full access to the user's access levels. Hackers often gain access using successful results from phishing attacks. (Wang et al., 2012) state that phishing is an email-based scam where a perpetrator camouflages emails to appear as a legitimate request for personal and sensitive information. More recently phishing attacks have also been referred to as "Spear Phishing Emails" in which more contextual information is used in the broadcast email in order to add more validity to the request. Often these use the contextual information to appear as though they have originated from an organisation of relevance to the user. Kaspersky antivirus software has detected around 200,000 phishing detections to fake Apple Computer websites between 2012 and 2013 (Kaspersky Labs, 2013). For users with no anti-virus protection in place there remains a significant risk to being exposed to phishing emails.

Figure 3 Access Control Model based on (Sandhu and Samarati, Pierangela, 1994, p.41)

Microsoft Corporation (2013) state that as the mobile Internet grows so does the volume of phishing impressions from mobile devices. Information gathered from Windows 8 mobiles shown in Figure 4 demonstrates significant attempts to target phishing attacks against financial and online services URL's. Microsoft deploy 'Smartfilter' technology in their browser which can check if the sites visited are known to be malicious and provide some level of warning but this is only against known phishing sites.

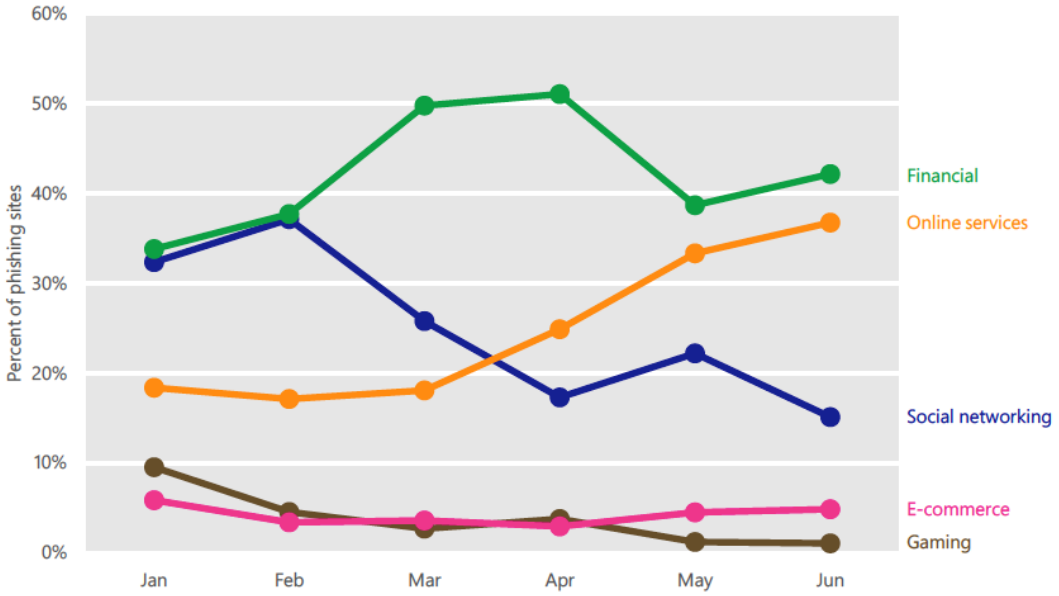


Figure 4 Unique phishing URL's visited by Internet Explorer on Windows Phone 8 January-June 2013 (Microsoft Corporation, 2013, p.96)

2.3.1 Identity Based Access Control (IBAC)

Identity based access control is a mechanism that uses the identity of the user to decide what resources they have access to and to what level. IBAC becomes complex to maintain within distributed cross-domain systems where multiple authentication processes may also be required (Hewlett PackardHP Laboratories Palo Alto, 2006).

2.3.2 Role Based Access Control (RBAC)

Role based access control is based on the type of role individual users carry out within their organisation (US Department of Commerce, 1992). This approach allows one set of access to a role rather than to the individual identity of the user.

2.3.3 Attribute Based Access Control (ABAC)

Attribute Based Access Control extended RBAC to allow context to be used for access such as time of day, or war vs peace (Karp et al., 2009). This model also reintroduced problems in multi-domain environments in which agreement was needed to identify these additional attributes.

2.3.4 Authorisation Based Access Control (ZBAC)

The ZBAC model attempts to make the process of passing authorisation requests between interconnected domains simpler and less prone to attacks (such as SQL injection attacks) by assigning certificates to the identity of the user along with the use of security assertion mark-up language (SAML) to effectively embed single sign on details (Karp et al., 2009).

All the preceding access control models focus on authentication being carried out and the resulting roles or identity assigned - ultimately allowing or denying access to resources. The physical location of a user does not appear to be considered in these models. Further consideration should be given to using location as an attribute in the ABAC model thus providing a new range of controls for where a user can or cannot access resources or services. For example, a user accessing a banking application may wish to check balances from any geographic location but only wish to access to transfer funds at home.

2.3.5 Location-Aware Role-Based Access Control (LRBAC)

LRBAC is an extension of RBAC in which location is considered in the model. Ray et al., (2006) demonstrate the model in Figure 5. The model allows for the role to be assigned only when a user is in the allowable predefined locations (i.e. A US Citizen would only be allowed to be assigned a role if they were physically in the USA). Similarly, a location-based role will only be activated when the user is in the accepted location (e.g. the role of audience in a theatre will only become active when the user is inside the theatre location) (*ibid)*.

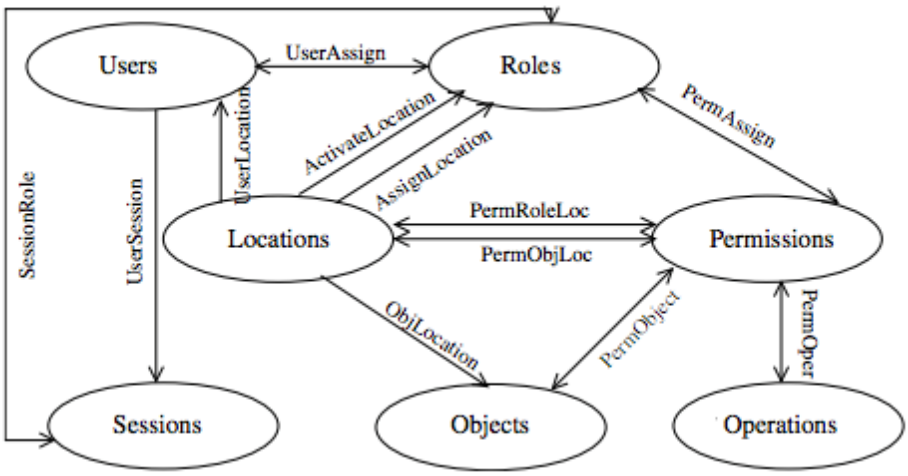


Figure 5 Relationship of RBAC entities with Location

2.4 Challenges in using Location on Smart-phones

Using location as a means to authenticate or authorise a user is not without significant risk. There are a number of attack vectors available to spoof GPS locations. Civilian GPS signals are not encrypted unlike the military GPS signal (U.S. Goverment, 2013). There are also privacy issues in relation to storing individual locations. This section will present the state of the art for this area.

2.4.1 GPS Blocking

GPS Blocking or Jamming is the process through which noise signal transmitted by a GPS hardware device concatenates with a GPS signal to create a new signal that a GPS receiver cannot understand. The result is a loss of signal on a GPS receiver within range (El-Bakry and Mastorakis, Nikos, 2009). The ubiquitous use of GPS across a range of transportation systems mean that there is significant risk to losing valuable positioning data. GPS Jammers are illegal to purchase in the US but not in the UK where ownership is not permitted yet purchasing has not been outlawed. GPS jammers are inexpensive and widely available. Although the lack of signal is effectively a denial of service it should become apparent that there is a problem due to the lack of positioning service to the device or user.

2.4.2 GPS Replay Attacks

Replay attacks are generated when a hacker records access control messages from another GPS device. They then replay this control message to gain access on a future occasion (Kannhavong et al., 2007). Replay attacks can be avoided by introducing a time stamp in conjunction with an asymmetric key. When the message is decrypted a comparison is made with the current time and if the gap is too long then the message is treated as suspicious and is rejected (*Ibid)*.

2.4.3 GPS Spoofing

Cavaleri, et al. (2010) describe GPS spoofing as the intentional transmission of misleading signals to GPS receivers fooling them to use counterfeit signals in space and compute erroneous positions. This is often achieved using GPS signal generators connected to a transmitting antenna (*ibid).* Warner & Johnston (2002) successfully tested GPS spoofing by broadcasting a stronger GPS signal to a truck to simulate legitimate GPS satellites. Once the receiver accepts the fake transmitter then false coordinates can be fed to the receiver without any knowledge that an attack had been made. This relatively early test was very limited in range as the truck had to be within 30 feet for the attack to be maintained.

In July 2013 the University of Texas carried out a similar test on board an $80 million yacht. A team from the university placed a GPS transmitter device aimed at the ships two receivers and once the GPS receiver accepted the broadcast as legitimate GPS transmitters they began receiving positioning data from the attack devices. The team were then able to fool the ships systems that they were a few degrees off course and the ship made a correction based on this incorrect data (Zaragoza, 2013).

2.4.4 Enhanced LOng-RAnge Navigation (eLORAN)

This vulnerability of GPS attacks to shipping transportation has been such a concern that an alternate positioning system called eLoran was developed. eLoran is a low frequency terrestrial navigation system based on a number of transmission stations (International Loran Association, 2007). eLoran is

designed to offer alternative positioning data to GNSS based systems such as GPS or the forthcoming European Galileo Satellite positioning service. In 2008 eLoran was tested off the coast of Flamborough Head (Grant, 2008). A ship had its GPS signal jammed. The installed eLoran system continued to operate to provide 95% accuracy up to 8.1metres.

eLoran technology is better than Global Navigation Satellite Services (GNSS) for resisting spoofing due to its signal strength being significantly stronger than broadcasts from GPS

2.4.5 Geoencryption with eLoran

QIU, Di et al. (2007) describe Geoencryption as the use of position navigation and time (PNT) information as a means to enhance the security of a traditional cryptographic system. This information is used to create a security verification tag that is needed to decrypt the data. It is suggested that the film industry would benefit from this approach to using location as a means of authorisation. For example, a geotag could be added to a film so that it can only be accessed at the cinema location at a particular time of transmission. This could reduce film theft as the encrypted film could be passed onto an unauthorised user who would be unable to decrypt the film to view the movie.

Whilst the process of geoencryption can help with the problem defined in this research it relies on a level of hardware (eLoran recievers etc) that is not currently part of mobile smartphone architecture.

2.4.6 Parking lot attacks

It is possible that an attacker could try to gain the correct geotag by trying to get as near as physically possible to the legitimate users location. This is known as “Parking Lot Attacks”. A counter measure to this is to use a 26 bit geotag. This approach, in conjunction with signal authentication, would result in an attacker having to try locations to identify the correct geotag (Qiu et al., 2007).

2.4.7 Geonencryption for mobile devices

Karimi & Kalantari (2011) propose a model for geoencrypting messages to mobile devices. This model outlined in Figure 6 is based on using the latitude and longitude values with the time and velocity values from the GPS receiver. These are combined using XOR and hashed to create a geo-tag value. The final stage is to combine with a session key to create a geo-secured key. In addition, the mobile application enables a user to enter a suitable dynamic tolerance distance (DTD). Once the receiver's location has been verified to be physically within the DTD then the user receiving the message can enter the session key to decrypt the message.

This model provides a model that can reduce the risk of attacks such as GPS spoofing, replay attacks and parking lot attacks. In order for the attacks to be reduced the RF navigation signal needs to be provided through message authentication in order to verify the source of the data or message. Section 2.4.8 outlines an alternative method of location verification. The challenge with this approach is the complexity for a typical end user. If the system is too difficult to use then the risk is that the end user will ignore this security layer.

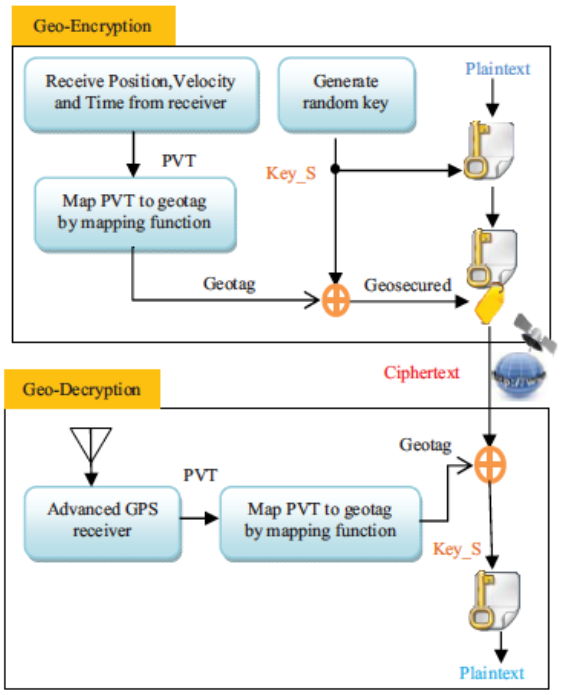


Figure 6 Encryption Model (Karimi & Kalantari, 2011)

2.4.8 Location Verification - SAGA

Becker, et al. (2010) propose a mechanism to verify the GPS location called Secure Authentication for GNSS Applications. This is a mechanism that uses the encrypted military satellite signal to compare signals from multiple satellites. This is done without the need to decrypt the military signal. If a hacker was attempting to spoof a signal it would not compare. The hacker could also not generate the encrypted signal without knowledge of the military private key.

2.4.9 Privacy Issues

Luo & Hengartner (2010) propose the use of location proofs to verify the location position is accurate on the mobile device. The location proof is an electronic form of document that confirms the location at a certain point in time. The example usage presented in their research is hospital staff only having access to a record when their location is within the hospital grounds or even a specific department. Their model then makes use of hash values and cryptographic keys to ensure that the location proof does not disclose the users identification.

In order to implement a system that authorises services or transactions for a user with a mobile device a centralised database server would need to exist to store where, when and what can be accessed. It could therefore be argued that a user's privacy is being exposed to another service provider or that the security risk is simply being moved to another potentially vulnerable data system.

2.5 Applications using location

In 2013 a patent was granted to implement smartphone location as a means of authorisation for bank ATM withdrawls (Block, J. et al., 2013). The patent describes a process in which the bank card initatiates the authentication for the customer wishing to use a bank service in an ATM. Before the transaction is authorised the location of the user's smartphone's (which has been pre-

registered) is checked in relation to its proximity to the ATM. If the ATM and the smartphone are in the same proximity then the transaction is authorised.

This approach to using location as a means of authorisation can be used to reduce banking fraud. Even if a criminal has the card and PIN code he would also need the legitiamate user's smartphone to complete the fraudlent transaction.

Diwakar , G et al. (2013) were granted a patent under the original assignee Amazon Technologies inc for Location-aware transaction authorization. The patent details a series of processes whereby a mobile user can send payments to other mobile users via their mobile phone. Once a request has been sent a location check is made for both users. Predefined account proximity rules are applied to decide whether to authorise the transaction or refer the payee for further checks before passing the transaction for payment.

Grigg, M.D, et al. (2013) filed a patent under the orginal assignee of the Bank of America that uses location to offer some fraud protection at the point of sale. The patent describes a process through which a bank customer registers their smartphone with the bank. When the customer makes a card payment in a store a check is made to ensure the phone is in proximity of the store that the payment has been requested from. If the phone and store are in close proximity the transaction is processed else the transaction is rejected or passed for further referral checks.

Whilst location is being used to offer an additional layer of security to reduce card fraud, flexibility in the rules here would need to be considered. For example, what happens if a bank customer is out shopping yet they have left their smartphone at home, or the phone is out of charge? In this example secondary checks may be offered such as a phone call at the retailer to verify the customer identity. If the proposed systems are too inflexible then they risk being over restrictive preventing the customers buying goods or services.

Most of the applications in this section relate to the physical payments where the client is either at a cash machine or a store. There appears to be limited

or no service to enable e-related goods or services to be purchased securely using location as a means of authorisation.

A relatively new service aims to address electronic payments in 2014 (Keenan, 2013). The service removes the need to have any card details when paying for goods or services. Instead a series of screens will be presented to the user (Figure 7). The system relies on a two tier security system. A 5 digit code entered by the user in conjunction with digital security tokens. The approach taken by Zapp is to embed this within the users mobile banking applicaton. The user can see the funds available prior to purchase and the funds are transferred real–time direct to the merchant selling the goods or services.

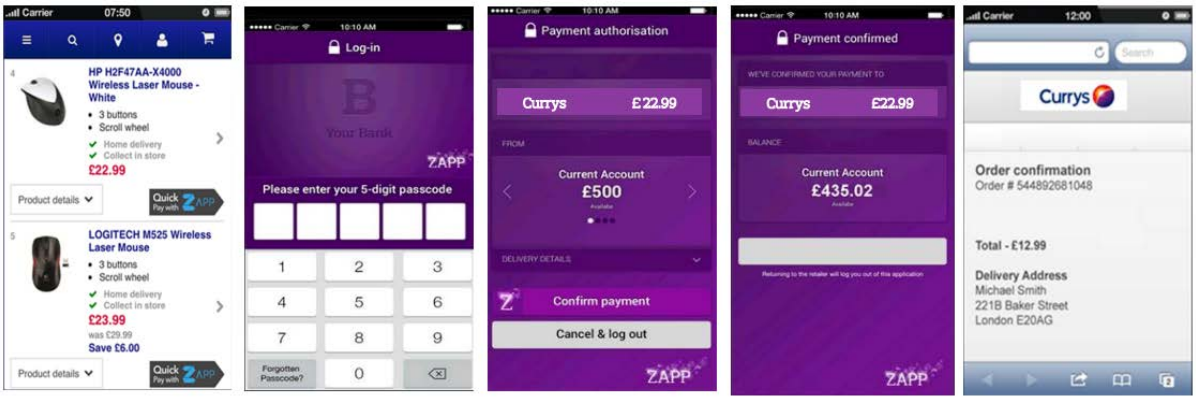


Figure 7. Payment process of the Zapp payment engine.

The focus of this application appears to be simplification of the checkout procedure. However, the user still has a single point of security info (i.e. a 5 digit code). Zapp do not detail the security token so its not possible to understand its risks. Positioning mobile payment systems within the bank system may satisfy users security concerns, however, there is no profile information of consumer spending habits built into the application utilising location information on the mobile device.

Financial regulations such as the US Anti Money Laundering require banks to identify and report customer money laundering activities or suspicious transactions (Price Waterhouse Coopers, 2011). It is not clear what level of detail the banks store for mobile transactions made. In order to use location as an additional authorisation method this metadata would be required to be

stored by the banks. Furthermore, there remains the issue of whether banking consumers would be comfortable with providing location data to their banks for spending habits.

The challenge with adding location into mobile payment applications relates to the interface presented to the user when paying and the ability for users to manage their own purchasing preferences, that are in turn utilised by payment applications. Research carried out within this thesis shows that location, as authorisation is not being considered as a means of authorisation by banks or retail merchants. The question of whether users want to restrict their mobile transactions this way remains unanswered. The current focus for mobile commerce transactions appears to be concerned with removing the need for bank debit cards for purchasing. Whilst this may be a positive step in encouraging more mobile commerce transactions, the issue of using a pin number only (as a form of authentication) solution still exposes users to risk. If location could be used at the point of sale as a form of authorisation then a more secure platform could be provided. The challenge is whether users are willing to engage with a service that uses location this way.

2.6 Users willingness to use location based technologies

In order for users location to be used as a means of authorisation they would need to be willing to use this approach and allow their location data to be stored in conjunction with their personal preferences.

Xu, Heng, et al. (2010) conducted a study of the decision making process for location-aware marketing. They created a conceptual model (Figure 8) that they used to survey users about their willingness to provide their location information in exchange for coupons from stores in their location. The model detailed a covert and overt approach. The covert approach was based on retailers monitoring the users location and providing offers when they were in close proximity to their store. The overt approach was based on a user request for coupons from a particular store similar to an on demand approach. Both these approaches were then assessed by the users perceived benefits against their perception of risk regarding information disclosure. The results

demonstrated that the “proposed impact of precious privacy experience on privacy risk was significant in the covert approach but insignificant in the overt approach” (Xu et al., 2010). The overall challenge from this research was that although the perceived risks were higher in the covert approach the resultant sales via issued coupons were higher.

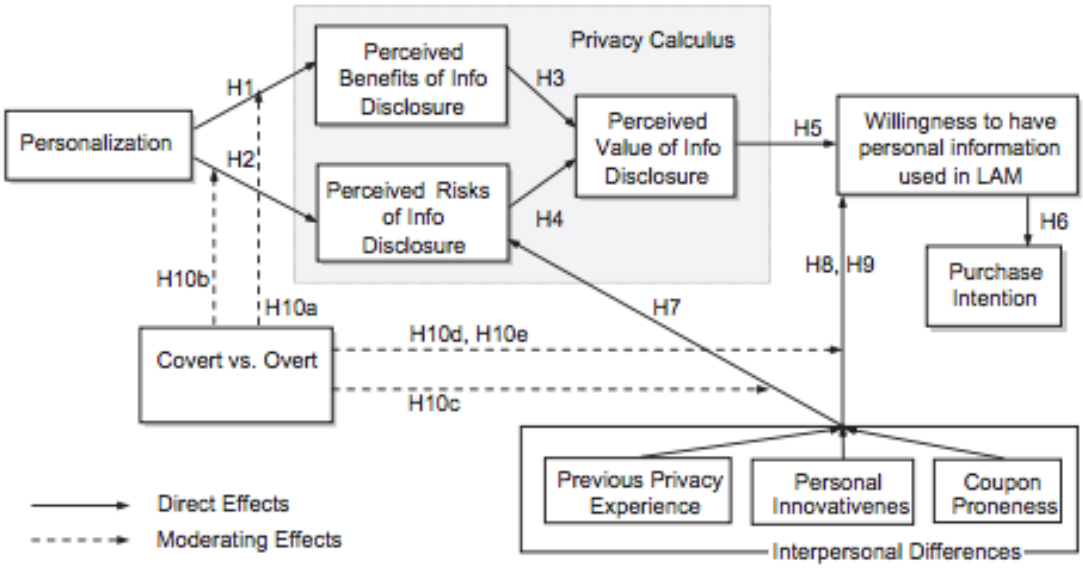


Figure 8. Conceptual Model for location-aware marketing Xu, Heng et al (2010).

LEON, Pedro Giovanni et al. (2013) conducted similar research into user willingness to share information with online advertisers. They found that users willingness to share personal information declined the longer the advertiser stored that information particularly if it was kept beyond a week. However, 53% of the users surveyed were happy to share their city and country location but only 4% were willing to share their exact location.

Stephens (2010) carried out research on the apple and android mobile devices. A number of applications were made available for download across a range of cateogories (Faith, Fun, Love, Philosophy and Science). Upon installing on android devices the user was presented with a screen informing them of the need to access device location prior to installing (Figure 9). The mobile

application was deployed both with permission requirements and then later without to see what affect it had on a user's willingness to engage and install the application.

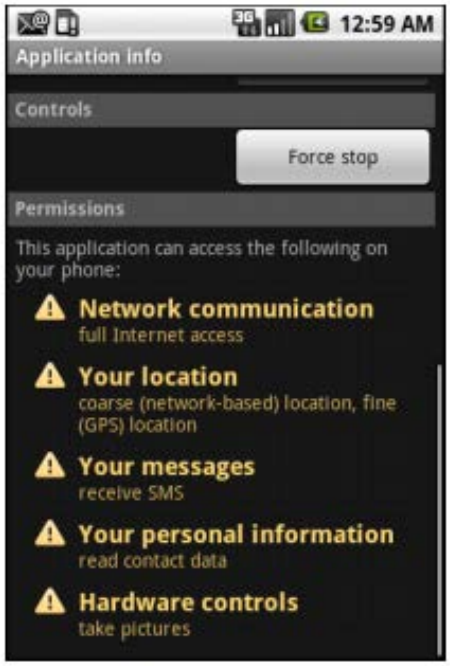


Figure 9. Screen shot of permissions screen (Stephens, 2010).

The results (Figure 10) show that the permission requests had little effect on user's willingness to install a third party application despite the unnecessary device intrusions. At the time of writing there appears to be no published research into user willingness to use location as a means of authorisation within the context of banking.

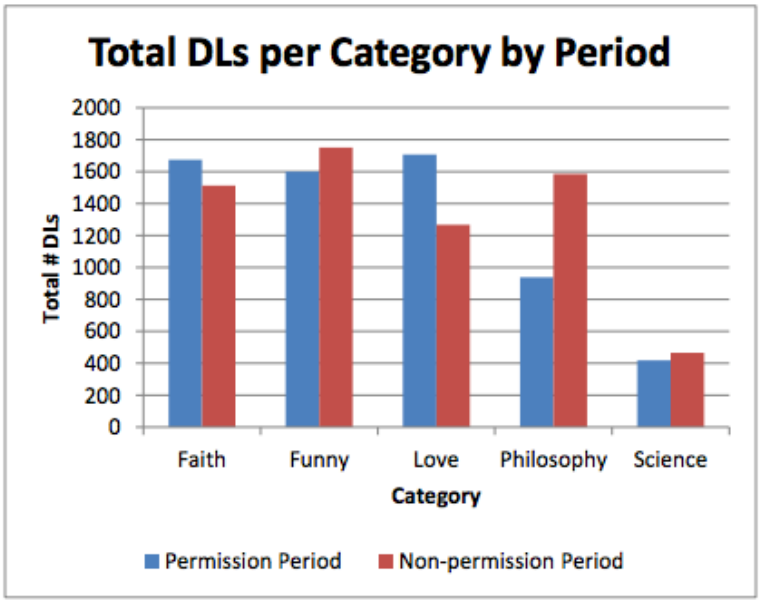


Figure 10. Total Downloads per category (Stephens. 2010)

This section demonstrates that users assess risk against potential value when sharing their personally identifiable information. Users appear less inclined to allow location information to be stored for more than a day. The context of the research is the sharing of information with advertisers. The risk value may differ when carrying out similar survey research within the context of banking transactions via their mobile devices. Further research is required to understand if users' concerns over allowing covert location positioning can be alleviated if they are given an interface to control over when and how this is used.

2.7 Problem Justification

This chapter demonstrates how services such as GPS and eLoran can be used to provide positioning information to a mobile device. Limitations exist as attackers can attempt to block or spoof a users position. Whilst services such as eLoran may offer an alternative more resilient positioning alternative, this service has yet to be offered to the consumer market for smart phone devices.

The research carried out in this chapter shows that there are still significant risks to mobile users particularly in the financial sector. As the mobile Internet grows so does the risk of phishing attacks.

Relying on positioning only as a means of authorisation may carry risk to the user but when used in addition to authentication methods it provides a more robust security foundation such as the model defined in Location Based Access Control in section 2.3.5.

The banking and retail sector are beginning to consider the use of smart phones as a means of authorisation both from an ATM and merchant services perspective, but research carried out does not show any significant research into the user acceptance of this model. The UTAUT provides a culmination of different user acceptance models into a single framework. This outlines different influences to users decisions to engage with new technologies. There appears to be very little research into the users acceptance of mobile authorisation within the financial sector but this framework will be useful for any customer survey and user experience analysis.

Whilst the technology appears to be either in existence in terms of location services such as GPS, eLoran and access control methods such as LBRAC or in development such as the authorisation patents outlined in section 2.5. A user's willingness to engage with such technologies does not appear to have been researched in any depth. The research carried out in section 2.6 suggests that there is a lack of understanding of what access third party mobile applications need when installing. Further research regarding the design of an interface to enable location-based controls within the banking sector is required.

In order to investigate a user's willingness to enable location-aware authorisation within the context of banking there is a need to carry out primary research of users. Qualitative methods would seem to offer the greatest opportunity to understand customer attitudes with respect to perceived values and risks.. The approach of embedding the mobile commerce transaction within existing banking mobile applications may alleviate user concerns over risk particularly if the users have some form of control within the banking application.

Chapter 3 User Acceptance Frameworks

The literature review in chapter 2 highlights the need to survey users to understand their willingness to use their mobile location as a means of authorisation. In order to carry out effective surveys, an analysis of current models of technology acceptance models is detailed in this Chapter.. A technology acceptance model offers a mechanism to understand how different types of users adapt to the use of new technologies, offering perspectives on which users are most likely to successfully adopt such technologies. This analysis is then used as a mechanism to to help formulate appropriate survey sections and hypotheses.

3.1 Current Models and Frameworks

There are a number of models that provide frameworks describing the different influences that effect a user's willingness to use new technologies.

3.1.2 Technology Acceptance Model (TAM)

This model illustrated in Figure 11 examines the perceived ease of use and also the perceived usefulness of the technology or system. The perceived ease of use is the degree that the person believes that using the system will make their job easier. The perceived usefulness is the degree to which a person thinks a system will enhance their job performance. Higher perceived usefulness and ease of use lead to a more positive attitude to the new technology system. The behavioural intention refers to what extent a user plans to perform or not perform a future action.

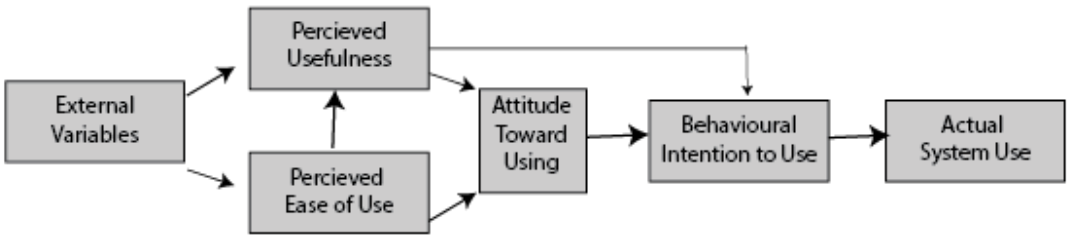


Figure 11 Technology Acceptance Model (Davis, 1989)

Davis stated that user perceptions can be affected by external variables. A lot of future acceptance models have expanded this earlier model.

3.1.3 Unified Theory of Acceptance and Use of Technology (UTAUT)

A number of different models were developed after Davis TAM in 1989. (Venkatesh et al., 2012) conducted empirical research into a number of these similar models in order to combine them into one model. They therefore developed a model to help understand users acceptance and the use of Information Technology illustrated in Figure 12. This model was initially developed in 2003 and extended later in 2012.

The model expands the external variables significantly into a number of different attributes. Performance expectancy is concerned with the level to which a user believes that using the system will help them with gains in their job performance. Effort expectancy is how easy the system is to use. Social influence is how the user perceives important that others believe they should use the new system. Facilitating conditions within the model relate to how supportive the organisational infrastructures are considered to be in order to support the use of the new system. These traits along with age and gender affect the behavioural intention and use behaviour in using the new system (Venkatesh et al., 2003).

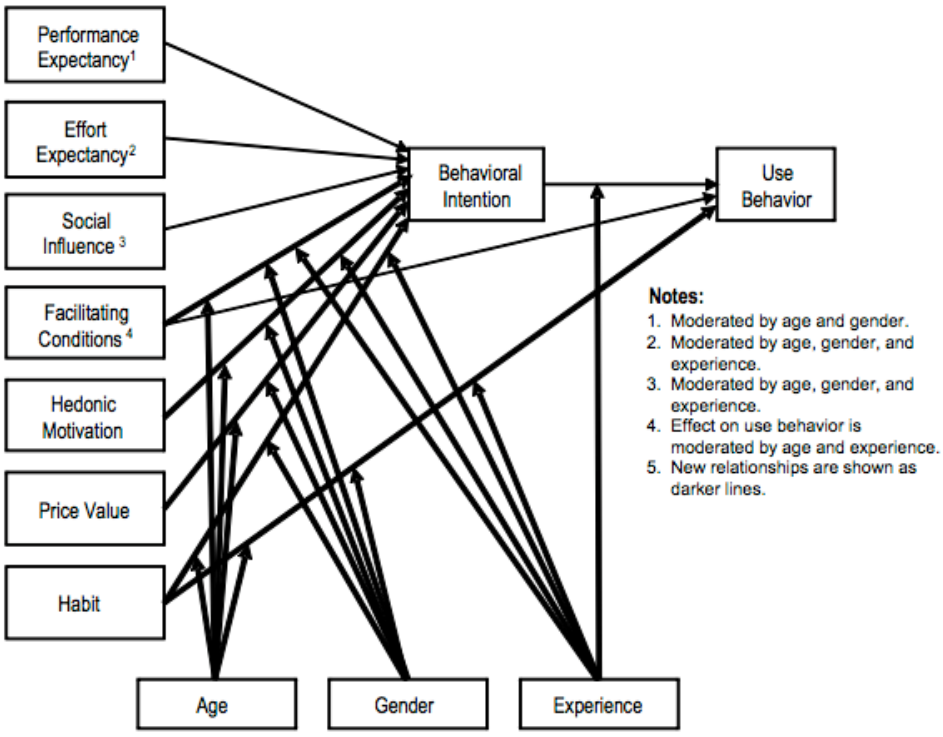


Figure 12 .An Illustration of the UTAUT2 model (Venkatesh et al., 2012)

The extended model in 2012 added Hedonic Motivation, Price Value Habit and Experience. The Hedonic Motivation is defined as the fun or pleasure the user derives from using the new system. Price factors have an affect on the use of the new system depending on the costs of alternative systems, particularly, if the user is a consumer and is personally responsible for the cost of using the system. Experience relates to the passage of time from first using the system and relates to the experiences of use as time passes. Habit relates to how the use of the new system becomes almost automatic and familiar to the user (Venkatesh et al., 2012). The models were tested with a study of consumers using mobile technology. The results demonstrated significant variations in influences in relation to the new constructs. An example is the use of watching multimedia on smart phones. The hedonic benefits of watching a movie on a small mobile screen may outweigh the costs of watching them.

This research appears to be aimed at business use and would need adapting slightly to consider personal users of applications such as those that fall under this research which may include both business and private users.

3.1.4 Applications of Models within Mobile Commerce.

An empirical examination of initial trust in mobile banking was carried out in China (Zhou, 2011). Usage of mobile banking applications was low and research was carried out via surveys in order to understand why usage was low. The TAM and UTAUT frameworks were reviewed and used in order to create a number of hypotheses' including perceived usefulness taken from TAM. The conclusion indicated, "structural assurance and information quality are the main factors affecting initial trust whereas both information quality and system quality affect perceived usefulness" (Zhou, 2011).

Zhou, Tao et al. (2010) used the Task Technology Fit Model to argue that users will adopt a technology based on the fit between the technology characteristics and task requirements. They also state that gender and education characteristics have significant effects on user adoption. They then use the TTF and UTUAT model to form individual hypothoses to evaluate mobile banking user adoption (Figure 13).

Additionally there was an empirical research conducted in mobile banking adoption within Portugal (OLIVEIRA, Tiago et al., 2014). The research area was in the same sphere of research as within this thesis. The research extensively used the UTAUT framework to relate survey data to user willingness to engage with mobile banking technology.

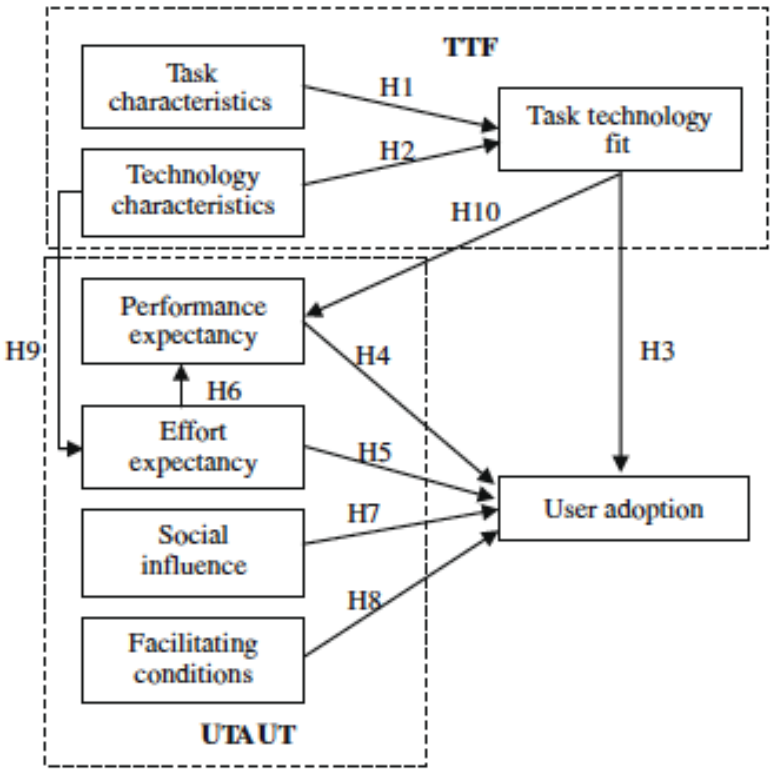


Figure 13. TTF and UTUAT Research model (Zhou et al. 2010)

Their conclusion states that a user's adoption of mobile banking is affected by the fit between their tasks and the mobile banking technology. This approach of combining the models allows the survey questions to be created and grouped against each hypothesis. User behaviour is dynamic and constantly changing so opinions can chage frequently. Past experiences do not appear to be factored into their model. For example, a user may have experienced financial fraud via a mobile or computer and this may directly affect a users willingness to engage with the techology or they may see it as an opportunity to reduce fraud.

3.1.5 Technology Diffusion Theory

Within the context of the frameworks consideration should be given to the type of user answering the survey. There is a socialogical model known as the diffusion theory that describes how a population adopts or rejects a particular innovation (Straub, 2009). Figure 14 graphically illustrates the cumulative frequency of the individual adoptions over time.

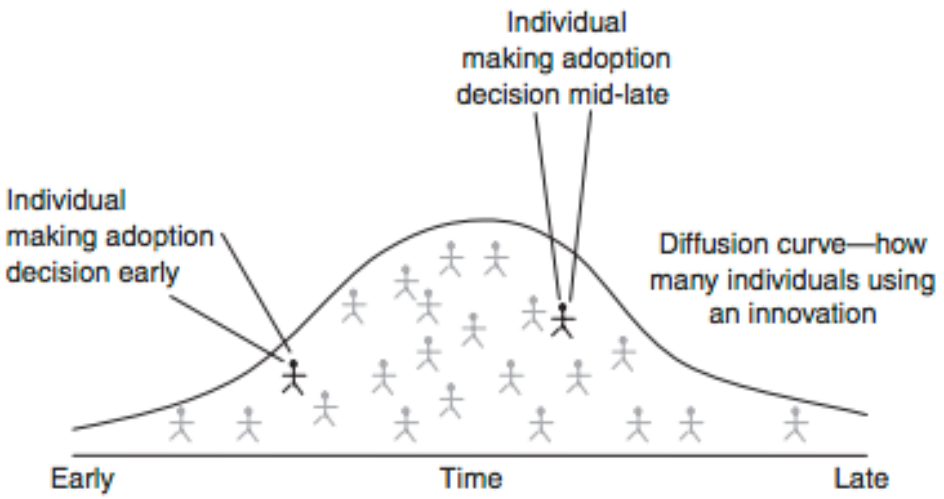


Figure 14 How Individual adoptions compose diffusion (Straub, 2009)

3.1.6 Technology Adoption Life Cycle

Earlier research by Moore (1991) focussed on the individual consumer types to describe the Techology Adoption Life Cycle (Figure 15).

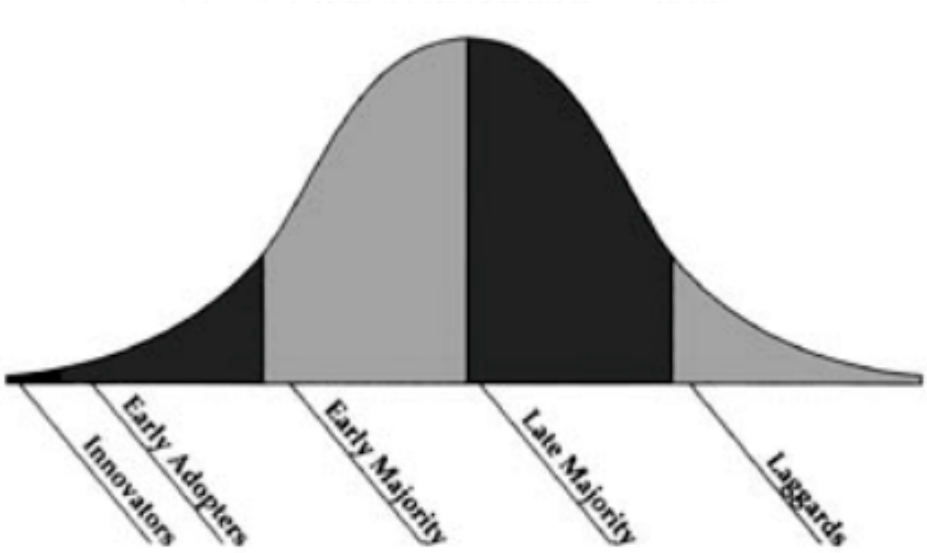


Figure 15 Technology Adoption Life Cycle ((Moore, 1991).).

He describes the first people to engage with technology as *Innovators*. These people pursue new techology aggressively due to it being a central interest in their life. *Early adopters* are similar to Innovators but they do not conisder themselves to be Techologists. They do find it easy to imagine the benefits of

using the new technology. The *Early Majority* are driven by a strong sense of practicality. They recognise that some technology releases are passing fads so wait and see how others use the techology before using themselves. The *Late Majority users* are similar to the Early Majority types except for one significant difference. The Late Majority are not entirely confident in their ability to use the technology effectively. They therefore wait until lots of support is available to assist them in using the new technology. The final type is the *Laggards*. They do not like new technology for personal and economic reasons. They typically only engage with the new technology when it is embedded inside another product (Moore, 1991).

3.2 Frameworks Summary and Conclusion

The models used for the TAM and UTAUT appear focussed on a user in a corporate or work environment. The addition of the Task Technology Fit model extends these models to a useful framework for this research on whether users will be willing to engage with device location technology as a means of authorisation. However, there are a number of background factors such as the ability to use technology that may be overlooked with these models alone. Any survey designed for this thesis will need to additionally consider:-

- The Type of User (From the Technology Adoption Life Cycle)
- Previous Fraud Experiences (Mobile based or pc based).

In addition, scenarios will need to be detailed in the survey to tease out influences on users decisions to use location-aware features in their mobile transactions using mock up mobile screen shots of transaction walk-throughs.

The UTAUT framework has been used in many research papers as a framework to relate hypothesis to research questions. (WILLIAMS, Michael et al., 2011) Stated that there had been 450 citations of this framework and considered whether this framework should be used at all. Their research identified that many researchers use elements of the framework rather than the complete framework and combine it with other similar user acceptance frameworks. They conclude that UTAUT provides a useful tool by which to

evaluate the potential for success of new technology initiation, and helps identify factors likely to influence adoption of technology. This extensive analysis of the use of the UTAUT framework support the approach taken in this thesis combining UTAUT framework with that of the Technology Adoption Lifecycle but also with consideration to users previous exposure to fraud.

3.3 Survey Purpose and Requirements

A user study in the form of a survey is required to understand whether users are ‘comfortable’ with allowing location to be used as a means of authorising transactions made via their mobile devices. Section 2.6 raises user concerns over covert location tracking. This can affect the users willingness to engage, however, the risk can be reduced if the user has control over when and how this monitoring takes place. A series of mobile device screen shots will be presented as part of the survey to show them how a mobile payment can be authorised using the location of the device. It will also show them the admin screens of how the user can control whether they wish to have this option on

and how to control it. Qualitative and Quantitative data will be collected and no personally identifiable data will be retained.

3.3.1 Hypothesis to be tested via surveys.

H1: Restricting mobile e-services using device location negatively affects the task technology fit. This is due to the perceived complexity to carry out the task on a mobile. The more complex the less the technology fit (Zhou et al., 2010).

H2: Embedding location-aware authorisation within existing mobile banking services makes it a better technology fit.

H3: Previous exposure to fraud makes location-aware authorisation a better performance expectancy.

H4 Later Majority user types find location-aware services increase the Effort Expectancy.

H5: Mobile devices should not be restricted by location.

H6: Mobile applications outside of the users current banking application that use location-aware authorisation lower trust.

H7: Storing location metadata significantly affects user adoption of location-aware authorisation.

H8: Education level affect effort expectancy for location-aware authorisation.

Hypothesis	Hypothesis Description	Relates to literature Review
H1	Restricting mobile e-services using device location	Section 3.1.4 relates to this hypothesis. There is

	negatively affects the task technology fit.	a risk that users will disengage with services using location restrictions if they perceive it too complex to use.
H2	Embedding location-aware authorisation within existing mobile banking services makes for a better technology fit.	Relates to Section 2.5 and 3.1.4. If the location-aware authorisation elements are embedded within current mobile banking services users will consider it a better task technology fit.
H3	Previous exposure to fraud gives location-aware authorisation a better performance expectancy.	Relates to section 3.1.3. People who have been exposed to fraud may consider location-aware authorisation as a means to better protect themselves from future fraud attempts.
H4	Later Majority user types find location-aware services increases the Effort Expectancy.	Relates to 3.1.6 and 3.1.4. Late majority users are not confident with their use of technology so may therefore find it too complex to engage with.
H5	Mobile devices should not be restricted by location.	This relates to section 2.6. Users may not be willing to restrict their devices. This can be tested against

		covert and overt monitoring of location.
H6	Banking applications that use location-aware authorisation increase trust.	This relates to section 2.6. There appears to be no research into the trust perception of location-aware restrictions based within banking applications and outside of them.
H7	Storing location metadata significantly affects user adoption of location-aware authorisation.	This relates to section 2.6. Users that have location data stored for any length of time can negatively affect users willingness to pass location data.
H8	Education level affects effort expectancy for location-aware authorisation.	This relates to section 3.1.4. The survey should test and relate education level to effort expectancy.
H9	Privacy concerns disengage users from making use of location-aware applications.	This relates to 2.4.9 Privacy Issues. The survey should test whether privacy concerns prevent users engaging with applications using location.

Table 2 Summary of how each hypothesis relate to the literature review.

Table 2 demonstrate how the hypothesis relates to the literature review sections. The overall aim is to explore consumers' perspective of mobile fraud protection and also the consumers' consideration to privacy in relation to location-aware services as detailed in section 1.3.

3.3.2 Survey Flow

Participants of the survey will be asked a series of background questions relating to age, gender, job role, education and some additional questions designed to try and understand if they fit into the categories detailed within the Technology Adoption Life Cycle. This information is important to understand if personal traits have any affect on the answers given and whether education levels affect response. Current phone make and models will be captured so that smartphone handsets can be identified. The number of devices users use to access mobile services via apps etc will be gathered such as tablet devices. It should then be possible to understand if participants have different security considerations according to the device they use.

Mobile Commerce will be defined and explained to the participants in order to provide context to a series of questions relating to their current shopping habits in relation to mobile purchases. Previous experience of fraud will be captured which relates to H3. This will enable data comparisons between users with fraud experience to those without. This section will also focus on the participants' attitudes to security relating to mobile devices enabling the testing of H5.

The next section will explain how device location could be used to restrict mobile commerce transactions. This will provide participants with context before asking questions about their perceived value of such restrictions. This will allow the testing of H1 and H4.

Finally a follow up section will request that users who would be happy to be contacted further leave their email contact address. This will allow a separate survey where a number of screen walkthroughs will be presented to the participants providing for further testing of user acceptance of restricting mobile commerce transactions by location.

Table 3 Survey to Hypothesis Relationship

Related Hypothesis	Question
Background Statistics	Please select your gender.

Background Statistics	Please select your age.
H8	Please select your highest education level
Background Statistics and to identify if job is in IT related.	Current Job
Background Statistics	What is your current phone make and model
Background Statistics To demonstrate to what extent users make use of application services using their smartphone.	Do you use your phone for the following Applications/Services:- • Mobile Banking • Ebay purchases • Amazon Purchases • Online shopping • Game Apps • Social Networking Apps • Foursquare • Sat Nav Applications • Maps
Background Statistics	Do you own a tablet device? If yes what make and model? Does your tablet have a SIM installed to enable you to use it away from a WIFI connection?
Background Statistics To demonstrate to what extent users make use of application services using their smartphone.	Do you use your Tablet for the following:- Applications/Services:- • Mobile Banking • Ebay purchases

	• Amazon Purchases • Online shopping • Game Apps • Social Networking Apps • Foursquare • Sat Nav Applications • Maps
	Your attitudes to technology:- Please state how much you agree or disagree with the following questions. Strongly Agree ☐ Agree ☐ Neither Agree or Disagree ☐ Disagree ☐ Strongly Disagree ☐
H4 (9-14)	When new mobile devices are released I make sure I purchase or upgrade as soon as possible.
	I feel technology is a central part of my life.
	When new mobiles and tablets are released I find it easy to understand the benefits of using the new devices.
	When new mobiles and tablets are released I often feel they are passing fads and prefer to wait and see how others use them before making a decision to use myself.
	When new mobiles and tablets are released I worry about my ability to utilise the new functions so wait until there is more help and support available.
	I have no interest in using the latest mobile and tablets.

Background to identify users who access banking services via mobile devices.	**Attitudes to Mobile Commerce**
	How often do you carry access your bank account via your mobile or tablet? • Once a day • More than once a day • once a week • never • other
	What activities do you carry out with your banking application on your devices? • Balance Enquiry • Bill Payment • Statement Enquiry
H3	Have you ever been victim to financial fraud? i.e. Card access, online access to bank or purchases without your consent?
H3	If yes please state the type of fraud with any details you are comfortable to share.
H3	Have you ever been a victim of a Phishing attack? If yes was that via an email received on a mobile device? If so please provide basic details.
Testing user perceptions of security between Desktop and Mobile platforms	Please state how much you agree or disagree with the following statement:- Accessing online banking and shopping is more secure on my desktop pc than a mobile or tablet.

H6	Do you use any applications that use your device location? If so what?
H5, H1	I find location services to complex to use.
H9	I am concerned about my privacy too much to consider using location services on mobile or tablet devices.
	Do you know how to customise location settings for mobile or tablet devices?
	If so, do you customise location settings for any applications that you are aware use the information? Why?
H5	Mobile devices and tablets should not be restricted by location at all.
H7, H2, H6	The ability to use device location within your banks mobile application to authorise different levels of access would make me trust the security of the application more.
H5, H7	If the bank stored my location data I would be less inclined to use it.

H5	Restricting where I can buy products and services on a mobile device or tablet would be too restrictive.
H3, H6	The ability to use location as a means to authorise mobile transactions would provide me with a better protection against fraud.
	Any other comments?

3.3.3 Pilot Survey Version 1

The design of this pilot survey is shown in Appendix A. It was tested on 10 candidates to test the question construction and the resultant answers. The pilot survey was carried out by sending a printed survey for users to complete.

3.3.4 Pilot Survey Results

There were a number of problems with the survey results. Only 2 out of 10 used their mobile for banking applications. This result meant that there was not much useful data to support this research.

The pilot survey also demonstrated that some of the focus of the questions related to the banking applications and not to online shopping.

3.3.5 Second Pilot Survey

The second pilot study was created and targeted only at people who use their mobile or tablet for online banking and mobile commerce transactions. The location-aware section was also expanded in the second pilot study to the ask the following additional questions:-

Table 4 Additional questions for second pilot survey

Related Hypothesis	Question

H1, H2. This also allows a basic test of user willingness to engage with an application that they can control the security settings.	Mobile devices and tables should only be restricted by location if I can control when and how this is setup.
H5. This also expands the test to see if users would use the proposed system if they could simply limit the area mobile transactions take place rather than a specific location (work, home etc).	I would be more interested in only restricting devices this way in the area I work and live (i.e. City/Town).

To make the survey easier to complete the open source survey framework Lime survey was installed and configured on a web server. This meant that questions could be dynamically displayed depending on answers given to previous questions. For example, if a user did not own a tablet then none of the questions relating to tablets would be presented to the user. This approach also enabled duplicate questioning of the Mobile Commerce section shown in Appendix B to identify if there were any differences to questions depending on whether the user was using a smartphone or a tablet device.

3.3.6 Second Pilot Survey Results

16 people responded to the second pilot study. It was apparent that some people completing the survey did not use devices for accessing banking or shopping services. This lead to a revised focus of the survey on users that do to ensure a significant relevant population was surveyed. Additionally the pilot survey did not separate mobile answers from tablet answers. The final survey was therefore modified as shown in Appendix C.

Chapter 4.0 Survey Analysis

This chapter details the main findings from the survey results show in Appendix D. 111 (Venkatesh et al., 2003) people responded to the survey.

4.1 Survey Background Results

48 (57%) of the survey respondents were female and 63 (48%) were male. This provides a reasonable mix of gender across the survey,

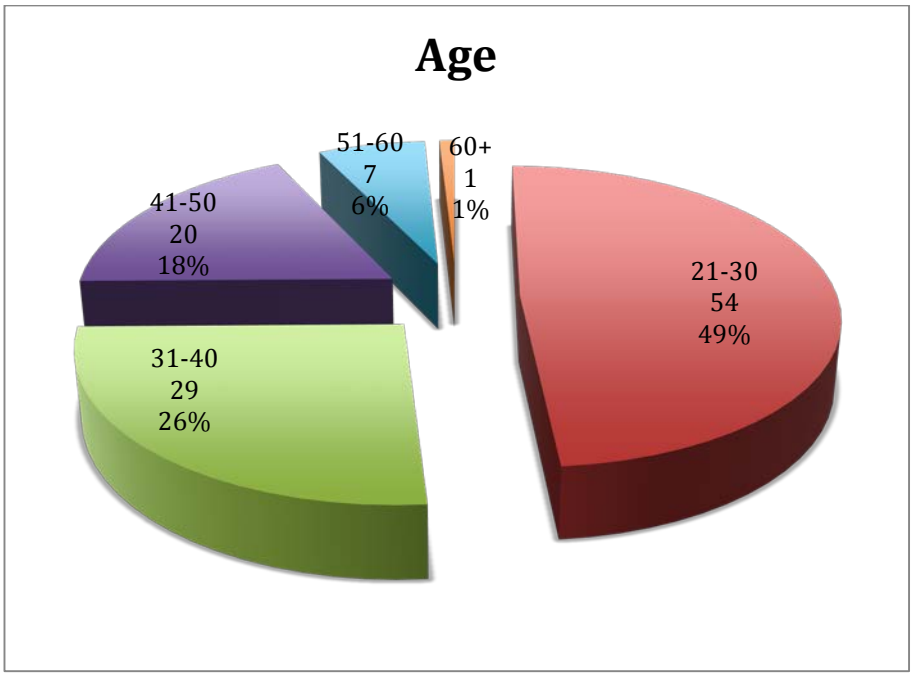


Figure 16 Age Range of Survey Respondents

Figure 16 shows the age mix of respondents. 54 (49%) of respondents were in the age group 21-30.

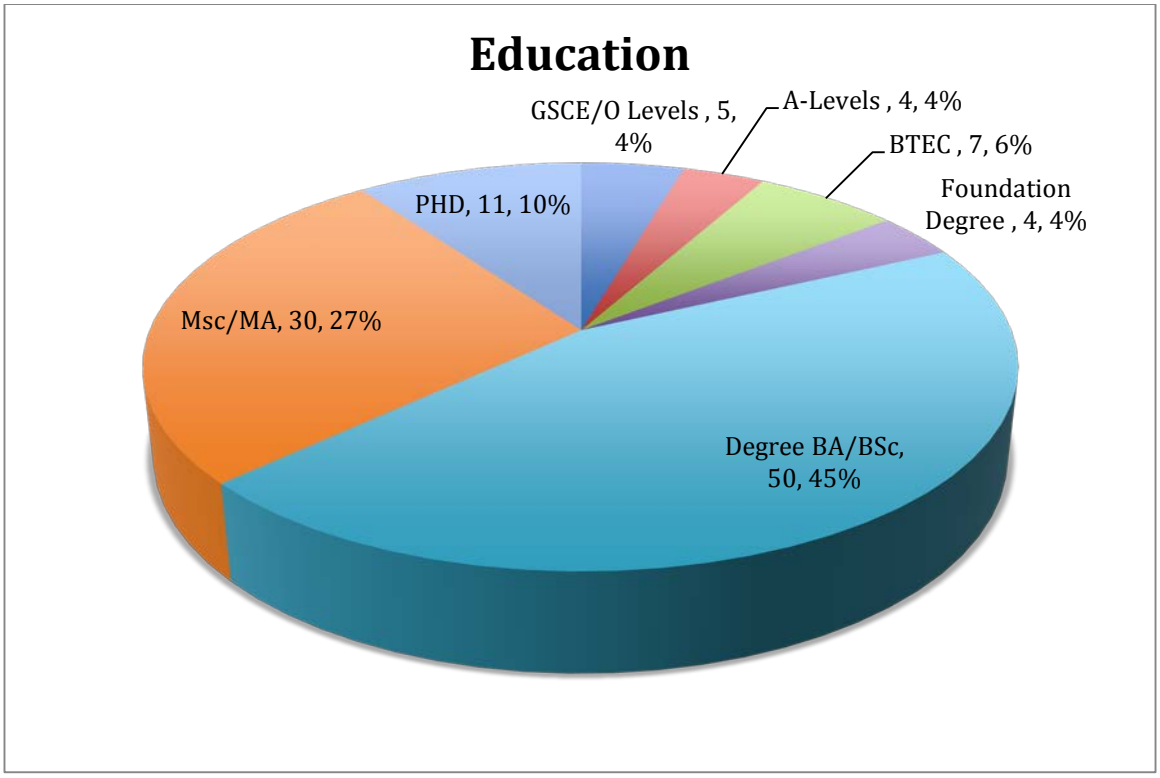


Figure 17 Education Levels of Respondents

Figure 17 shows the highest education level of the survey respondents. The majority of respondents (91, 78%) were degree level or higher.

4.2 Survey Results for Approaches to Technology

61% (68) of respondents owned a tablet device. Figure 18 shows the services used by respondents on both mobile and tablet devices. In terms of m-commerce, more people use mobiles for mobile banking than tablet devices (61.26% Mobile Users as opposed to 52.94% of tablet owners). However in terms of shopping, a higher percentage of respondents that own tablet devices use their tablet for shopping online (69.12% of tablet users carry out online shopping as opposed to 57.66% of mobile users). The same trend follows through for eBay purchases. 45.95% of mobile users purchase from eBay via their mobile device as opposed to 52.94% of tablet owners.

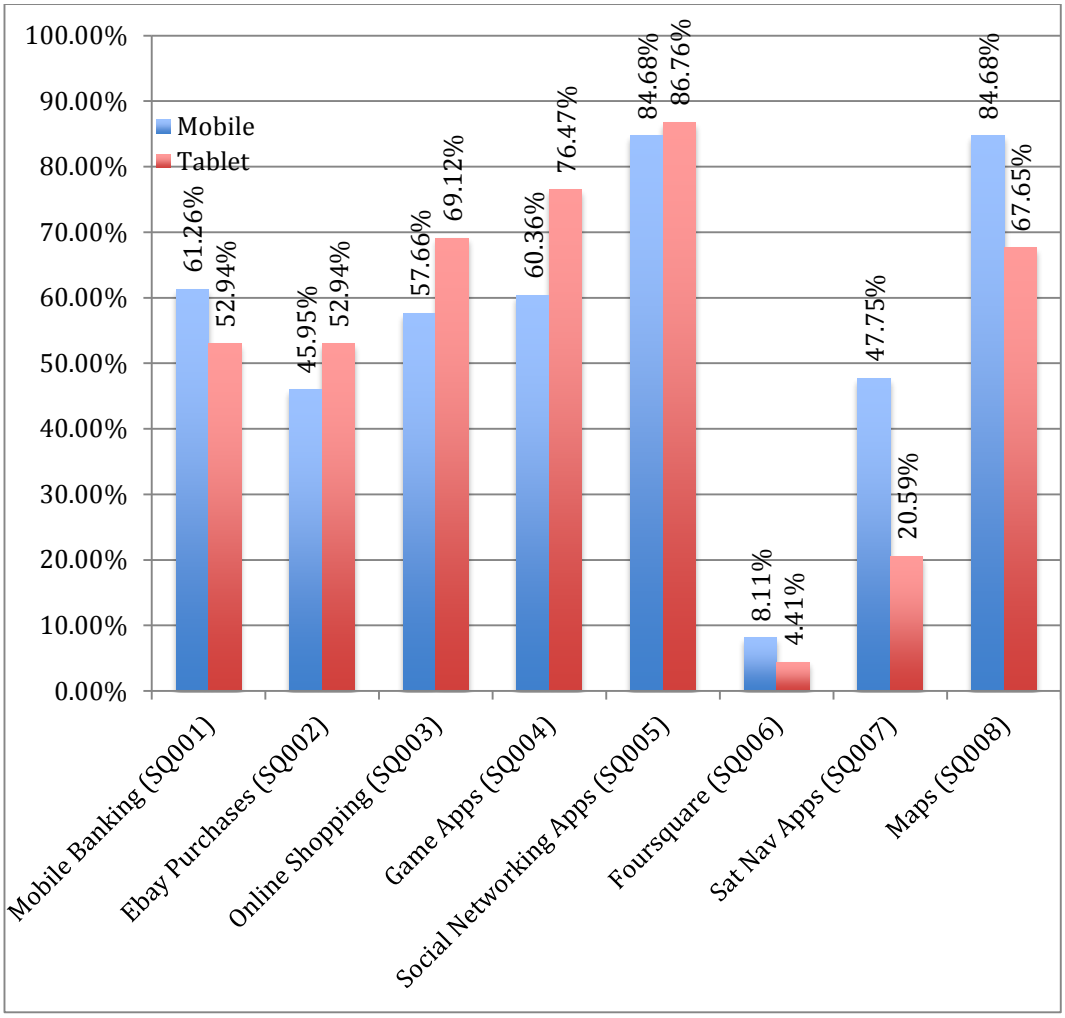


Figure 18 Services Used By Device Type

This section of the survey asked respondents about their attitudes to technology to identify what type of user they were according to the Technology Adoption Lifecycle shown in section 3.1.6. The results are shown in Figure 19 and are displayed by taking the response “Agree” or “Strongly Agree” from questions 9-24 in Appendix A. The results of the survey differ slightly to the original model proposed in section 3.1.6 where most respondents identify with the early adopter role as opposed to the Early Majority role in the original model. Respondents did however identify with more than one role by answering favourably to more than one question in the group.

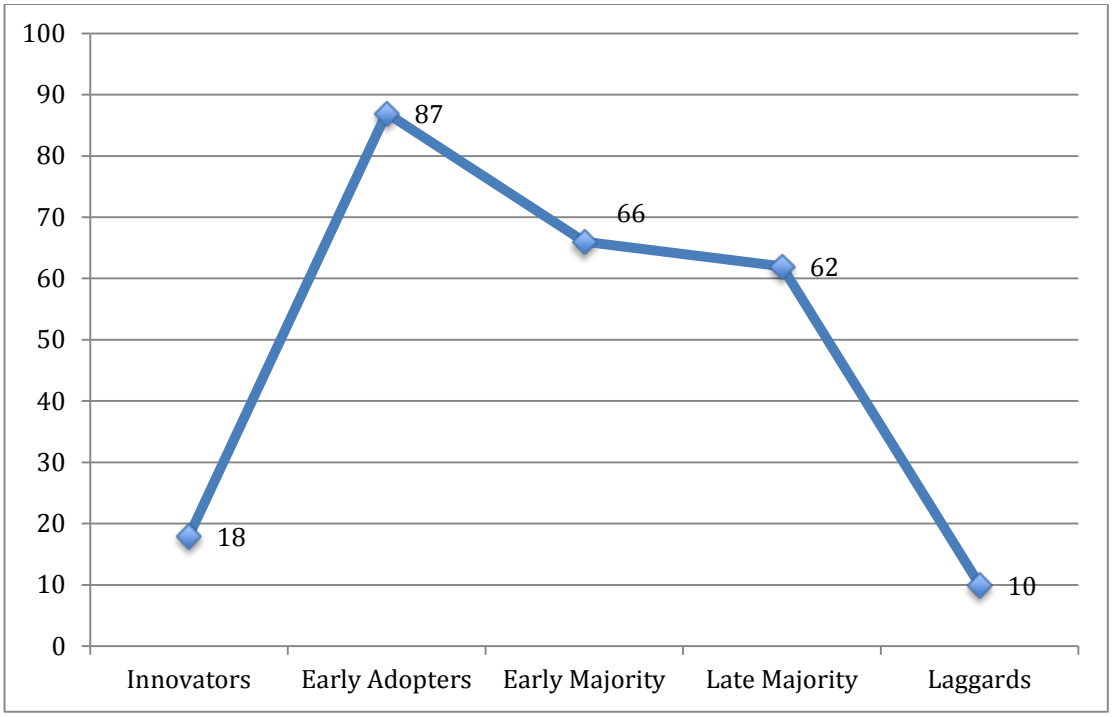


Figure 19 Technology Adoption Lifecycle Types from Survey

Respondents access online banking mainly once a week both on mobile and tablet devices (54.4% Via Mobiles, 50% via Tablets). Balance Enquiry and Statement Enquiry were the most accessed service within banking access. 92.65% of mobile users that access online banking access banking balance enquiry as opposed to 94.44% who access the same service via tablets. 47% of mobile users that access banking services use statement enquiry as opposed to 58.33% on a tablet.

4.3 Survey Results for Mobile Commerce

Table 5 Respondents that Access Banking and Online Shopping via Tablet or Mobile

Location	Banking Services		Shopping Online	
	Mobile	Tablet	Mobile	Tablet
Home	58.82%	86.11%	45.31%	97.87%
Work, School/College/University	48.53%	33.33%	28.13%	23.40%
On way to work	23.53%	5.56%	4.69%	2.13%
Anywhere	70.59%	19.44%	37.50%	21.28%

Table 5 shows the percentage of respondents that access banking or shopping online via a mobile or tablet. Clearly most respondents (70.59%) access banking services from their mobile anywhere whereas tablet users mainly access banking services from home. Online shopping differs in that 45% of users who carry out online shopping via their mobile closely followed by 37.5% shopping from any location. Clearly there is a mix of locations people access these services. Tablet online purchases happen mainly at home but respondents still reported also shopping online via tablets at work and also from any location.

10.81% of survey respondents (12) claimed to have been victim of financial fraud. Qualitative responses collated show that the fraud types were mainly card detail theft including fraud attempts from overseas. In some instances banks fraud detection systems prevented the fraud taking place. However, in some cases fraudulent transactions were made against the victims account and were only spotted when the victim later checked their bank statements.

When asked if accessing online banking and shopping is more secure on their desktop pc than a mobile or tablet,(41.44%) stated that they neither agreed nor disagreed with this statement. This suggests that users are not necessarily apprehensive in terms of security for these services compared to carrying out the same activities on desktop pc.

4.4 Survey Results for Location-aware

The survey responses show a clear awareness of “Location Services” on tablets and mobiles with 92.79% declaring their awareness of this service. Indeed 73.87% of survey respondents are aware that they use applications that make use of their location. Qualitative responses were captured listing the applications respondents used with location. The responses were a mix of social media, mapping, health and discount applications. 63.06% of respondents declared that they do not find location services to be hard to use.

Privacy concerns with location showed a split response. 35.04% of survey respondents are concerned too much about their privacy to consider using location services on mobile or tablets. 24.32% neither agreed nor disagreed whereas 39.64% were not concerned about their privacy too much to use location services.

59.46% of survey respondents customise location settings but a significant 40.54% does not. When asked why they do not customise location settings the majority stated that it was too much effort or that they did not feel the need to. One response stated that “If someone in a position of power ever needs to find me, me changing my location services won't stop that. Also my devices are used predominantly over encrypted Wi-Fi so I'm not overly concerned about cyber crime” this demonstrates some users lack of understanding of how crime can affect them within a mobile device. Encrypting the data does not prevent a user from a phishing attack for example.

37% of respondents agreed or strongly agreed that mobile devices should not be restricted by location at all. However, the majority (74.77%) strongly agreed or agreed that they should only be restricted if they can control how this was setup. When asked if they would be interested in only restricting to the town or city they work and live, 44.14% expressed an indifferent response neither agreeing nor disagreeing. 35.13% said they would be interested as opposed to 20.22% that were not interested in this approach.

When asked if the ability to use device location within the users mobile banking application authorising different levels of access would make them trust the application more, 45.05% agreed or strongly agreed. This demonstrates that there is significant user interest from the survey respondents in using location within m-commerce to help reduce fraud. 18.92% either disagreed or strongly disagreed with the remaining population (36%) being indifferent to this question. Further research to understand the indifference reasons would add value to this area of research.

Restricting where users can buy goods or services on devices highlighted the respondents' opinions that this would be too restrictive. 68.48% declared that this approach would be too restrictive. However 41.44% of respondents agreed that the ability to use location as a means to authorise transactions would provide them with better fraud protection.

4.5 Hypothesis Test Results

Table 3 demonstrates how the survey questions relate to each hypothesis. This section presents the results of each hypothesis.

4.5.1 Hypothesis 1 Test Results

Hypothesis 1 states that Restricting mobile e-services using location negatively affect the task technology fit. The Task Technology Fit Model states that users will adopt a technology based on the fit between the technology characteristics and task requirements . The survey asked users whether they consider location services too complex to use. Only a small percentage (3.6%) of respondents agree or strongly agree with this statement. The question used in the survey related to location services in general rather than location services linked to financial transactions.

4.5.2 Hypothesis 2 Test Results

Hypothesis 2 states that embedding location-aware authorisation within existing mobile banking services makes for a better technology fit.

45.05% agreed or strongly agreed that the ability to use a device's location within your banks mobile application to authorise different levels of access would make them trust the security of the application more. This suggests that there is significant sample that support this hypothesis however 36% were indifferent. Similar questions will be asked after a design prototype walkthrough is shown to a smaller focus group to see if there are any differences.

4.5.3 Hypothesis 3 Test Results

This hypothesis states that previous exposure to fraud gives location-aware authorisation a better performance expectancy. Of the 111 survey population 12 (10.81%) claimed to have been a victim of financial fraud.

Performance expectancy is concerned with the level to which a user believes that using the system will help them with gains in their job performance (Venkatesh et al., 2012). The survey is concerned with consumers rather than corporate workers. In this instance job performance relates to carrying out user tasks more effectively.

Table 6 . Survey responses from users previously affected by financial fraud.

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
Mobile devices and tablets should not be restricted by location at all.		41.67%	41.67%	8.33%	8.33%
Mobile devices and tables should only be restricted by location if I can control when and how this is setup.		25%	58.33%	16.67%	
I would be more interested in only restricting devices this way in the area I work and live (i.e. City/Town).		50%	33.33%	16.67%	
The ability to use device location within		50%	33.33%	16.67%	

your banks mobile application to authorise different levels of access would make me trust the security of the application more.					
Restricting where I can buy products and services on a mobile device or tablet would be too restrictive.		50%	25%	25%	
The ability to use location as a means to authorise mobile transactions would provide me with a better protection against fraud.		41.67%	33.33%	16.67%	

There appeared to be no significant difference in percentage results of the complete survey population. The final question on better protection against fraud resulted in 41.67% agreeing with this question. The results therefore show no significant difference in responses for those affected by fraud and therefore disproves this hypothesis.

4.5.4 Hypothesis 4 Test Results

This hypothesis states that Later Majority user types find location-aware services increases the Effort Expectancy. When filtering the survey results on Late Majority types this shows that 40% of Late Majority types do not find location services too complex to use and 60% neither agreed nor disagreed.

This is a contrast to the overall responses in that 63.06% of users disagreed or strongly disagreed that location services were too complex to use. Whilst an indifferent response could be argued that late majority consider location services too much effort to engage with. Further testing with a more detailed example is needed to verify this.

4.5.5 Hypothesis 5 Test Results

This hypothesis states that mobile devices should not be restricted by location. 38.74% agreed or strongly agreed with this statement. Most response (45.05%) neither agreed nor disagreed with this statement. This suggests that the hypothesis is not proven.

4.5.6 Hypothesis 6 Test Results

This hypothesis states that banking applications that use location-aware authorisation increase trust. The survey population were asked if the ability to use a device's location within their banks mobile application to authorise different levels of access would make them trust the application more. 47.05% agreed or strongly agreed with this statement. Similarly, when asked if they thought such a system would better protect them against fraud, 61.44% agreed with that statement.

4.5.7 Hypothesis 7 Test Results

This hypothesis states that storing metadata significantly affects user adoption of location-aware authorisation. 40.54% of respondents agreed or strongly agreed with this statement. 28.83% disagreed or strongly agreed and the highest individual response (30.63%) was from respondents that neither agreed, nor disagreed, with this statement. Clearly storing data splits opinions on whether they use the application with a significant amount claiming they would be put off by such an application. However, those people may change their opinions based on whether they consider the fraud protections worth using within the application.

4.5.8 Hypothesis 8 Test Results

This hypothesis states that the user's educational level affects effort expectancy for location-aware authorisation. When comparing the results of respondents with education levels lower than degree there were sufficient results to disprove this hypothesis. When asked if they found location-services too complex to use, 68.75% disagreed or strongly disagreed. This was similar to levels from the complete population (61.53%).

4.5.9 Hypothesis 9 Test Results

This hypothesis states that privacy concerns disengage users. 36.04% agreed or strongly agreed that they were concerned about their privacy too much to consider using location-aware services on mobile or tablet devices. 39.64% disagreed with this statement. A higher number of respondents therefore disagreed with this hypothesis although by a small margin.

4.6 Problem Justification

Section 4.5 demonstrates that users are willing to engage with location-aware services on devices. A significant amount are still willing use such services despite privacy concerns. Most users do not find location-services too complex to use. They also believe that the ability to use location as a means to authorise mobile transactions would provide them with a better protection against fraud.

The survey asked a question relating to location-services in general. The responses support a smaller survey that can show users how a location-aware service may help them to better protect themselves against mobile fraud. This will enable a better understanding of how users choose to engage with location-aware services in the context of mobile commerce rather than from a general viewpoint.

5.0 Location-aware Application Design

This thesis is concerned with understanding user acceptance of a location-aware mobile commerce application. In order to further analyse this, in this Chapter the design of an application to enable location-based authorisation for online banking services is provided. The design will enable a subset of the original survey group to walkthrough the application; understand how it may work, and feedback on its perceived usefulness. This will allow a better understanding of user acceptance of this approach. The design of the screens relate to the original survey and the answers given to make for a more engaging design.

5.1 Device Mock-up Screen Designs

The assumption for the design is that the application will form part of the users current mobile banking application as 45.05% of respondents from the original survey agreed or strongly agreed that the ability to use the device location within their banks mobile application to authorise different levels of access would make them trust the security of the application more. This approach will enable testing of the effect of positioning the menu within the banking application. The design screens are based on the iPhone, however, the functionality used is also available on other devices.

5.1.1 Main Menu Design

Figure 20 shows a mock up screen for how the main menu might look for location-based security. This screen provides simple links to adding a device, services and locations. 38.74% of the survey population stated that they believed that mobile devices should not be restricted by location. Taking this into account the screen shows three potential options: -

- Device restriction based authorisation
- Location restriction based authorisation
- Both Device and Location based authorisation

This can be achieved by simply switching commonly used toggle switches (in green) on or off from this menu.

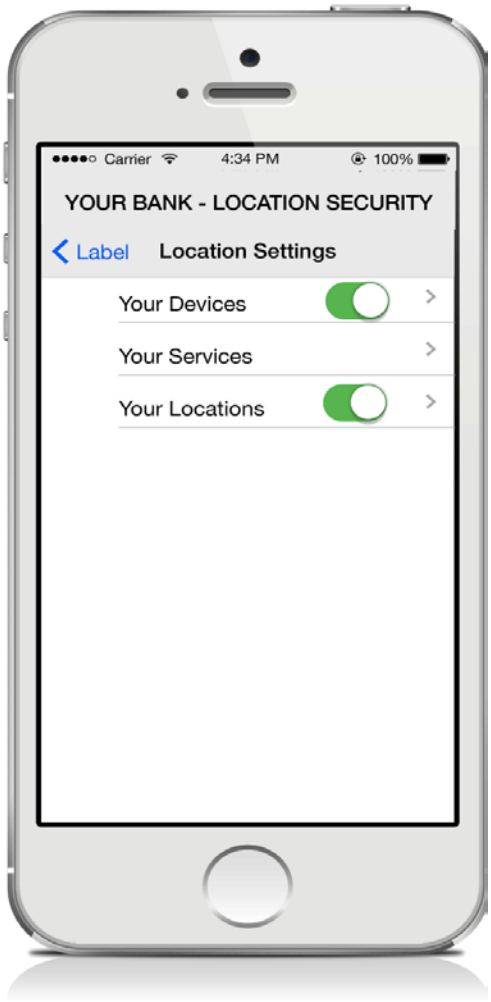


Figure 20 Location Settings Menu Screen

5.1.2 Device Control Screens

The devices screens shown in Figure 21 show the controls to add devices to the application. This would provide the flexibility of enabling or disabling individual devices using simple iPhone toggle controls. The method of identifying and verifying the individual devices is via a locally installed certificate. When device authorisation is enabled the certificate would be used to verify the device before authorising the transaction.

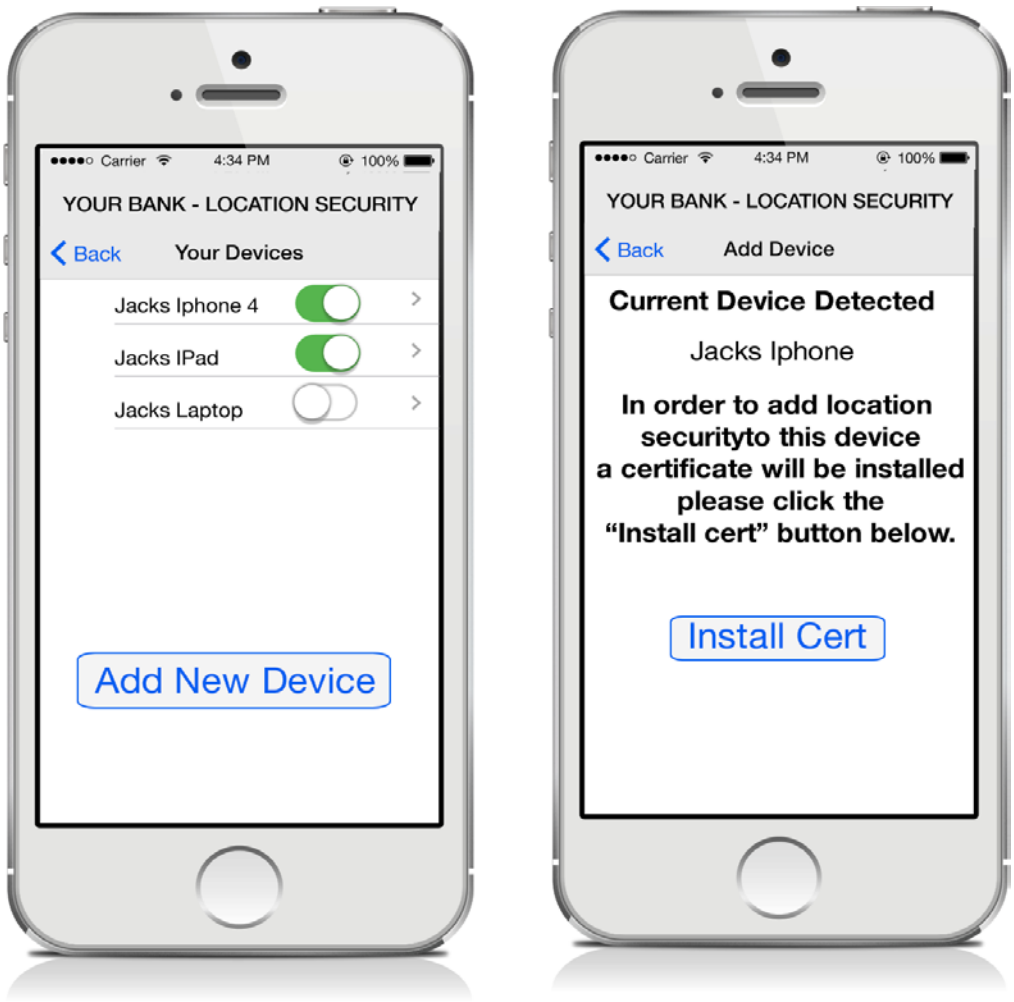


Figure 21 Device Control Screens

5.1.3 Service Screen

Figure 22 shows the proposed layout for the services screen. The design is based on the survey feedback regarding the applications which users make the most use of online within mobile banking, and also in mobile commerce via tablets and mobiles. There are a number of options here that can be customised. This design has been constructed as a result of the survey majority (74.77%) agreeing that devices should only be restricted if they can control how this setup. The screen is setup with two sections. One service screen aimed at controlling what banking services can be used and the other aimed at mobile purchases.

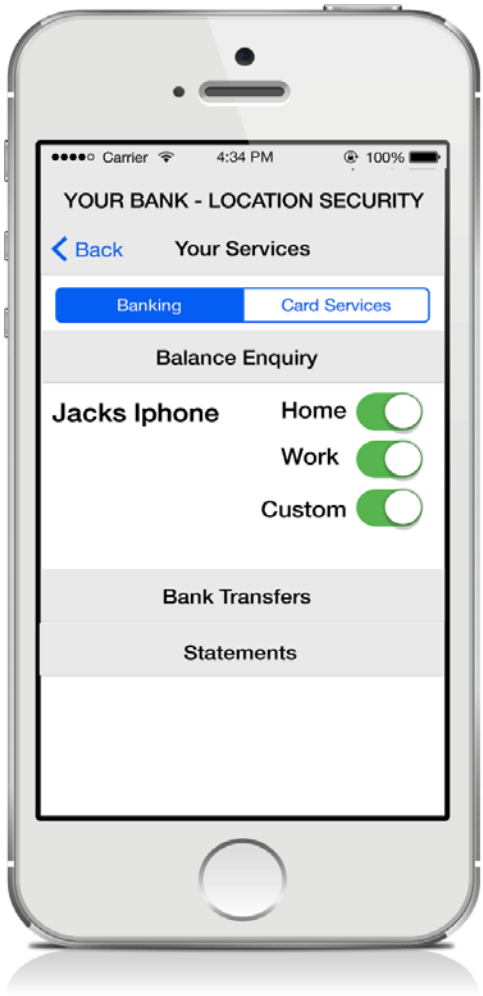


Figure 22 Service Screen Layouts

The banking screen will consist of banking features a user can carry out in terms of online banking functionality. Each service would be accessed via collapsible accordion style responses i.e. User touches the Bank Transfer option and the balance enquiry section would collapse and the bank transfer would expand. Within each banking activity the user would have control over which devices can or cannot access the service by location per device.

The card services section would have the same structure but would have the ability to control PayPal payments, debit cards, credit cards etc. in the same way. Toggle buttons provide user control over restrictions.

5.1.4 Location Setting Screens

Figure 23 shows the design mock up for setting up possible user locations to use within the service screens. In this example three options are available:-

- Home
- Work
- Custom – This is the option to define an area not previously covered by home or work.

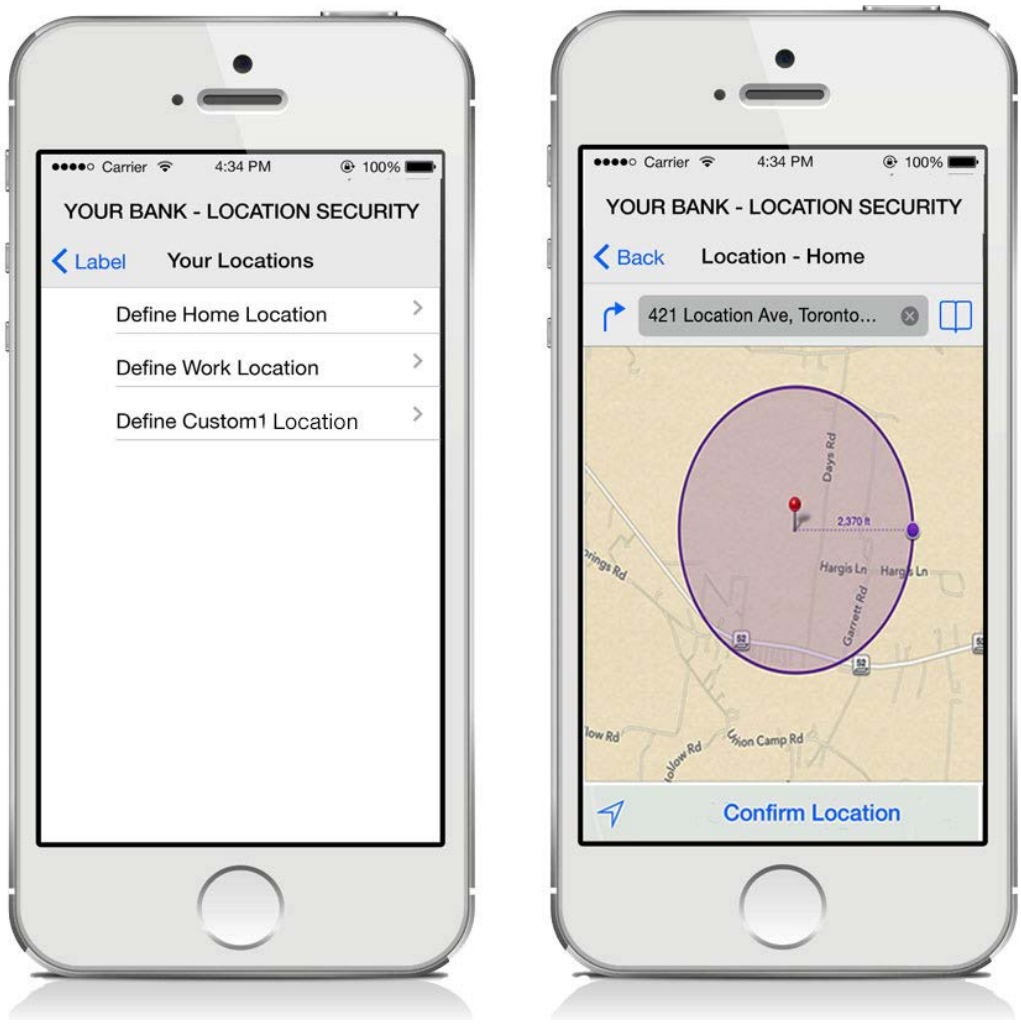


Figure 23 Location Setting Screens

When you select any of the three options you are taken to the map screen where you can use common device functions to find your present location or indeed set others. When you have identified the centre of your location a radius around the point will be displayed. This will allow users to use gesture

controls such as pinch and zoom to set the approximate area they wish to include in the defined location. There could be a potential problem in simply dropping a single point in the map, as the resultant GPS positioning may not be accurate enough to work correctly. Once the user is happy with the circle then they touch the confirm location button at the bottom of the screen.

5.2 Secondary Questionnaire Design

36 people from the original survey agreed to take part in a secondary survey. The secondary survey population were sent the screens of the application (See Appendix D) with explanations of what each screen does and the functionality each provides. They were then sent a link to an online survey using the open source survey tool Lime Survey.

5.2.1 Survey Questions

Table 7 shows the survey questions designed and how they relate to the original hypotheses'. Not all the questions have a direct correlation as they are aimed more at the potential usability of the application.

Table 7. Application Survey Related to Hypothesis

Question	Related Hypothesis
Location may be useful in limiting fraud in ecommerce transactions.	
If this system was implemented in my banking application I would find it simple to understand and use.	H1
This application would be too complex for me to bother using.	H1, H3
The ability of toggling device and/or location controls makes me likely to use as I can control the settings.	H1
Adding Devices	

The process of adding devices appears too complex to use or would make me less likely to bother using the application.	H1
The ability to toggle on/off individual devices registered makes the application more useful to me.	
Services	
Restricting banking services per device in conjunction with location appears complicated and I wouldn't understand how to use this.	H1
I would prefer to simply allow or disallow mobile banking over individual features.	
Restricting services by location only would be enough for me rather than per device.	
If my bank had to store my locations and devices to use this system I believe the fraud protection it offers me would be a greater benefit than the privacy concerns I may have about my location data.	H5, H6
Defining my locations with pinch gesture controls seems simple enough to use.	
Would you use a similar system to this if your bank offered it? Please add any comments.	
If my bank offered better fraud protection benefits as a result of	H6

using this system would you consider using it?	
If this application was separate too your banking application I would trust it less.	
If the bank stored and analysed my usage data I would still use this application for the fraud protection benefits.	H7
I am too concerned about privacy issues to consider using an application like this.	H9

Chapter 6.0 – Application Survey Results

This chapter details the main findings from the application survey results shown in Appendix E. A smaller focus group of 20 respondents from the original survey took part in this survey.

6.1 – Application Results

Table 8 shows the results from the second survey. The responses are shown against each question and the percentage of the respondents displayed underneath.

Table 8. Application Survey Results

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
Location may be useful in limiting fraud in ecommerce transactions.		17 (85%)	1 (5%)	2 (10%)	
Device usage may be useful in limiting fraud in ecommerce transactions.	1 (5%)	15 (75%)	4 (20%)		
The ability of toggling device and/or location controls makes me likely to use as I can easily control the settings.	7 (35%)	9 (45%)	4 (20%)		
The process of adding devices appears too complex to use or would make me less	1 (5%)	2 (10%)	2 (10%)	11 (55%)	4 (20%)

likely to bother using the application.					
The ability to toggle on/off individual devices registered makes the application more useful to me.	7 (35%)	10 (50%)	3 (15%)		
Restricting banking services per device in conjunction with location appears complicated and I wouldn't understand how to use this.	2 (10%)		1 (5%)	13 (65%)	4 (20%)
I would prefer to simply allow or disallow mobile banking over individual features.	1 (5%)	3 (15%)	6 (30%)	9 (45%)	1 (5%)
Restricting services by location only would be enough for me rather than per device.	1 (5%)	4 (20%)	6 (30%)	9 (45%)	
If my bank had to store my locations and devices to use this system I believe the fraud protection it offers me would be a greater benefit than the privacy concerns I may have about my location data.	1 (5%)	11 (55%)	5 (25%)	1 (5%)	2 (10%)

Defining my locations with pinch gesture controls seems simple enough to use.	6 (30%)	10 (50%)	3 (15%)	1 (5%)	
Would you use a similar system to this if your bank offered it?	1 (5%)	17 (85%)	1 (5%)	1 (5%)	
If my bank offered better fraud protection benefits as a result of using this system I would consider using it.	4 (20%)	15 (75%)		1 (5%)	
If this application was separate to your banking application I would trust it less.	5 (25%)	8 (40%)	5 (25%)	2 (10%)	
If the bank stored and analysed my usage data I would still use this application for the fraud protection benefits.	1 (5%)	10 (50%)	5 (25%)	4 (20%)	
I am too concerned about privacy issues to consider using an application like this.	1 (5%)	1 (5%)	5 (25%)	9 (45%)	4 (20%)
If this system was implemented in my banking application I would find it simple to understand and use.	4 (20%)	11 (55%)	4 (20%)		1 (5%)

This application would be too complex for me to bother using.	1 (5%)	1 (5%)		12 (60%)	6 (30%)
I can see the usefulness in using location this way to help reduce fraud in my transactions.	1 (5%)	16 (80%)	2 (10%)	1 (5%)	
Using device controls seen in the proposed application to limit fraud attempts would be useful.	1 (5%)	15 (75%)	3 (15%)	1 (5%)	

6.2 – Application Survey Analysis

The first two questions in the application survey were asked prior to seeing the application designs. This was to gauge if there were any differences before and after seeing the survey. 85% of respondents agreed that location may be useful in limiting fraud in ecommerce transactions. Furthermore, 80% either strongly agreed or agreed that device usage may be useful in limiting fraud in ecommerce transactions. This demonstrates that users can see the value in this additional layer of security.

In the initial survey (74.77%) strongly agreed or agreed that they should only be restricted on their devices if they can control how this is setup. The designs of the application reflect this with the introduction of toggle controls. This approach resulted in 80% of respondents agreeing that this would make it a more customisable application. In addition, 85% of respondents agree that the ability to use toggle controls to turn off individual devices would make the application more useful to them.

The challenge of designing the application was whether it would be perceived as too complex for users to engage with. There were a number of questions

relating to this area within the second survey. When adding devices, 75% of respondents did not feel it was too complex for them to bother using. Additionally, 85% of respondents did not feel the banking service restrictions were too complex for them to use. Defining locations was also reported as easy to use with 80% agreeing that the gesture controls were simple enough. 75% of respondents felt that the application overall was simple to understand and use. 90% did not feel the application was too complex to bother using. This demonstrates user willingness to engage with this level of security.

Users were asked if they would prefer a simplified alternative whereby they disable services in general but the responses show that 50% disagreed that this would be a preferable alternative. Only 20% agreed with this approach.

Privacy concerns were not sufficient against the fraud protections offered in the approach of this application. 60% of respondents considered the benefits of fraud protection higher than the privacy concerns they had about location data being stored. Furthermore, 65% of respondents were not too concerned about privacy issues to use an application like this. If users were offered better fraud protection benefits as a result of using an application like this, then 90% stated that they would use the system. Clearly the banks could provide more incentives to make an application like this more widely accepted.

Users were also asked if they would trust the application any less if it was not part of the banking application. 65% agreed that they would trust it less outside of the banking application. This clearly shows that the nature of financial protections should be promoted via the banking sector in order to be more widely accepted by consumers.

90% of respondents agreed that they would use an application similar to this if the bank were to offer it to them.

At the end of the survey users were asked similarly worded questions to those asked prior to viewing the application design screens. The results were identical responses suggesting that the application did not change user's perceptions on fraud protection in this manner.

6.3 – Application Survey Hypothesis Results

Table 7 demonstrates how the survey questions relate to each hypothesis where appropriate. This section presents the results of each hypothesis.

6.3.1 Hypothesis 1 Test Results

Hypothesis 1 states that Restricting mobile e-services using location negatively affects the task technology fit. The Task Technology Fit Model states that users will adopt a technology based on the fit between the technology characteristics and task requirements . The survey asked users whether they consider location services too complex to use. 90% of the respondents stated they would consider using an application like this to provide an additional layer of security based on their location which disproves this Hypothesis. Using location would not therefore negatively affect the task technology fit.

6.3.2 Hypothesis 2 Test Results

Hypothesis 2 states that embedding location-aware authorisation within existing mobile banking services makes for a better technology fit.

In the initial survey 45.05% agreed or strongly agreed that the ability to use a device's location within their bank's mobile application to authorise different levels of access would make then trust the security of the application more. This suggests that there is significant sample that prove this hypothesis however 36% were indifferent.

In the application survey, users were asked if they would trust the approach less if it sat outside of the banking application. 65% agreed that they would trust the application less. Overall 90% of respondents stated that they would use an application like this as an extension to their mobile banking.

6.3.3 Hypothesis 3 Test Results

This hypothesis has already been disproven in section 4.5.3 and is not relevant to the second survey.

6.3.4 Hypothesis 4 Test Results

This hypothesis was relevant to the first survey only.

6.3.5 Hypothesis 5 Test Results

This hypothesis states that mobile devices should not be restricted by location. In the first survey 38.74% agreed or strongly agreed with this statement. The highest response (45.05%) neither agreed nor disagreed with this statement. This suggested that this hypothesis was unproven. However the second survey results show that 90% of respondents would use the application if their banks offered it to them. Providing the visual ideas of the example application may have been sufficient to persuade people that location restrictions could be a good thing when considered in relation to fraud protection. There is sufficient evidence to disprove this theory. A larger survey population would however, provide more weight to this argument.

6.3.6 Hypothesis 6 Test Results

This hypothesis states that banking applications that use location-aware authorisation increase trust. The original survey population were asked if the ability to use the device's location within their banks mobile application to authorise different levels of access would make them trust the application more. 47.05% agreed or strongly agreed with this statement. Similarly, when asked if they thought such as system would better protect them against fraud, 61.44% agreed with that statement. There was sufficient data in the original survey to prove this hypothesis. The second survey results supported this further by presenting visuals as to how the different levels of restrictions could be controlled by the user. When asked if they wanted to reduce the amount of levels of restrictions to simply restricting mobile banking as a service, 50% disagreed with that approach.

6.3.7 Hypothesis 7 Test Results

This hypothesis states that storing metadata significantly affects user adoption of location-aware authorisation. In the original survey 40.54% of respondents agreed or strongly agreed with this statement. 28.83% disagreed or strongly agreed and the highest individual response (30.63%) was from respondents

that neither agreed nor disagreed with this statement. Clearly storing data splits opinions on whether they use the application with a significant amount claiming they would be put off by such an application. However, once users had been shown the functionality of the application 60% of respondents agreed that the fraud protections provided by such an application outweigh the privacy concerns. Whilst storing metadata does affect user adoption of location security, providing context to a working model appears to be sufficient to disprove this hypothesis.

6.3.8 Hypothesis 8 Test Results

This hypothesis relates to the original survey only.

6.3.9 Hypothesis 9 Test Results

This hypothesis states that privacy concerns disengage users. In the original survey 36.04% agreed or strongly agreed that they were concerned about their privacy too much to consider using location-aware services on mobile or tablet devices. 39.64% disagreed with this statement.

In the second survey, users were asked if they considered the benefits of fraud protection would outweigh the privacy concerns when using the application. 60% of respondents agreed with this statement providing a more significant response to disprove this hypothesis.

7.0 Limitations of Research

It is important to note that there are some limitations relating to the research. This section identifies known limitations in order for future research to address the limitations that have taken place.

70% of the survey population was gathered by mailing the survey to current University Postgraduate Students. Gathering respondents from a range of sources could have produced a more balanced survey population in order to test the hypothesis in a more diversified manner. Future research in this area should concentrate on non-academic population in order to compare and contrast the resultant data.

The age range categories shown in Figure 16 show a significant age category within the 21-30 category. This section of respondents account for 49% of the survey population. Similar research should concentrate on different age categories to identify any differences in responses.

There is a limitation in the approach taken for the application design. This research is focused on a user interface without extensive consideration to the underlying technical banking infrastructure required. This approach was important to allow the focus to be on the user willingness to engage with the location-based security processes from an interface perspective. Although the results were positive in terms of user willingness to engage, further research including a banking sector partner will enable more technical focused research to understand the feasibility of the proposed interface from this thesis.

Chapter 7 – Analysis of Results

This thesis has explored user willingness to use location to reduce fraud attempts on their devices. A broader survey was carried out to gauge overall user opinions

7.1 Users Understanding of Location Technology

Users were asked about their current understanding of location services within applications and their use. There were clear indications from both surveys that users do not find location services too complex to engage with. The first survey question was too generic with a focus on location services as a whole rather than relating to financial transactions. The example shown to users in the second survey after viewing the application demonstrated that 90% of respondents were willing and comfortable with using an application like this. There is therefore clear indication to support the task technology model described in section 3.1.4 Applications of Models within Mobile Commerce. The results show that making use of familiar controls i.e. Phone controls such as Toggle buttons help improve the task technology fit.

7.2 Trust and Privacy

Providing user controls to enable personalised security also increased trust levels with 45.05% of respondents agreeing with this approach. Section 4.5.6 demonstrates that users agree that the use of device location within their banks mobile application increases their trust level. This was further supported after demonstrating how an example banking application would work. After seeing the example application users were asked if they would prefer a simpler system. 50% disagreed with that approach. This study shows that as long as an application using location security measures had user controls then they would both trust the application more and also be more inclined to use it.

The responses in table 8 show that users would trust the example application less if it was not embedded in their banking application. 65% agreed or strongly agreed with this statement.

There were some concerns with banks storing data for location settings in terms of privacy. However, section 6.3.7 demonstrates that users were initially

concerned with privacy when banks stored metadata around their location usage. After viewing the application 60% of respondents agreed that the fraud protections provided by such an application outweigh their privacy concerns.

7.3 Performance and Effort Expectancy

The UTAUT model in section 3.1.3 states that performance expectancy is concerned with the level to which a user believes that using the system will help them with gains in their job performance. Within the context of a consumer environment the users need to understand how the location controls would help them better protect them against financial fraud. The results from the survey with user controls demonstrate that the example application is worth the respondents using as they perceive that it would better protect them against fraud.

Effort expectancy is how easy the system is to use. By making use of common phone features such as the toggle functionality this study has demonstrated that respondents would find this system simple enough to use. 90% of respondents in the second survey disagreed that the system would be too complex to use.

7.4 Design Concept Discussion

7.4.1 Location Services

The sample application shown in chapter 5.0 allows users to select a radius on a map to define their location. This is achieved by first selecting the centre of the location to be defined. The user using gesture controls as shown in figure 23 then adjusts a circular area to the area they wish to cover. The application would then need to geo-encode the area sending the values to the banking database. These values would then be used as a comparison for future transactions. If location controls were in effect then the transactions for that device would only be allowed if they were within the defined area. This would create a further challenge to a hacker in that they would need to spoof the locations defined in order to gain access.

The approach taken could be additionally hardened from spoof attacks if systems such as eLoran detailed in section 2.4.4 were used to verify the position of the device.

The application does enable a broad sweep level of authorisation across all user devices for the services specified. Clearly the participants in the survey are happy to engage with this approach as long as it is embedded within their banking application controls.

7.4.2 Device Controls

In order to apply different location settings for different devices the application would require the use of certificates to verify the validity of the device. This would allow comparative checks when transactions take place in order to allow or deny the transaction. If the device controls were used this way then this may also prevent hackers using location spoofing as they would still require a valid certificate for the device placing the transaction.

7.4.3 Application Positioning

Users looking at the sample application indicated that they would overcome privacy concerns if the application were embedded in the bank application controls. However, it may be preferable to position it within the card providers layer i.e. Visa or MasterCard. This approach may enable the check to occur at the stage currently seen in the Verified By Visa screens seen when purchasing online (Figure 24).

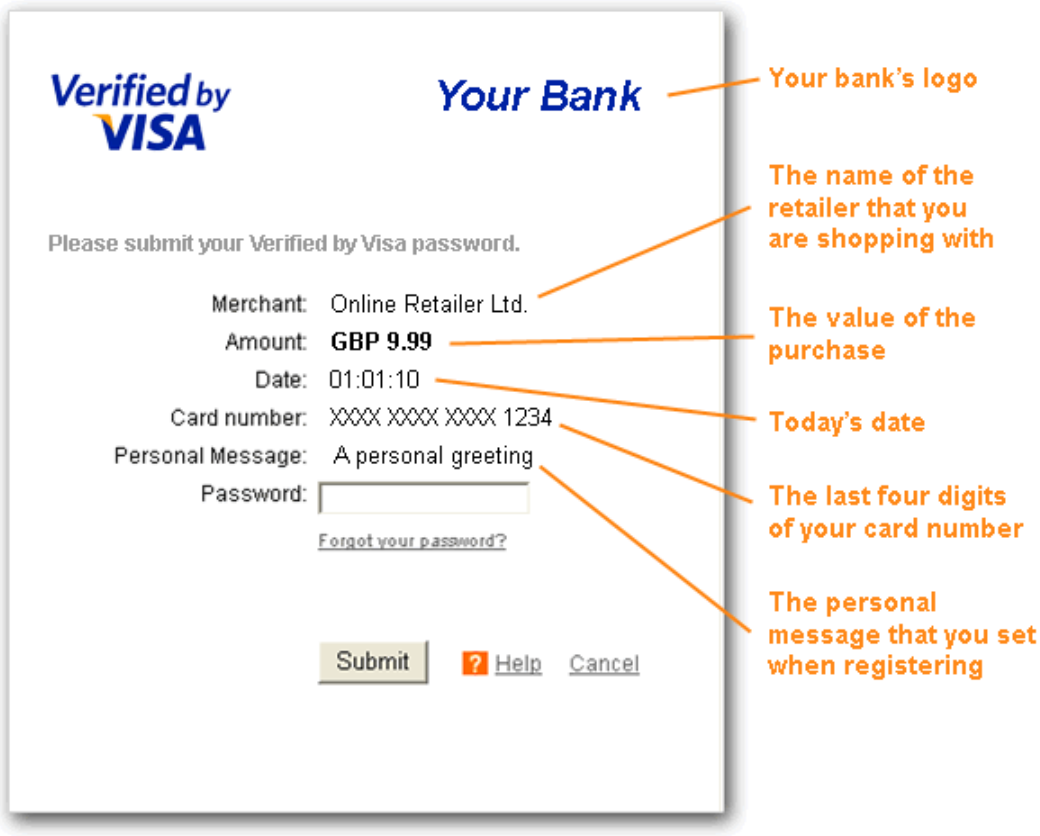


Figure 24 Current Example of Verified By Visa Page (Visa Europe Ltd, 2014)

Embedding the application checks at the Visa level could be achieved with the check taking place when this screen appears. An additional Line could be displayed “Location Authorised” or “Location not authorised”.

7.4.4 Query Load Testing

This research is focussed on the user acceptance of location authorisation. Whilst users appear to be willing to engage with the application security controls proposed it may be problematic in terms of the time taken to check device and location and then approve or deny.

Chapter 8 - Conclusion

This research has investigated whether location-aware technologies can be used to provide additional layers of security within ecommerce transactions. A review of the state of the art for location-aware technologies was carried out along with potential problems with location-aware technologies.

An online survey was carried out asking users opinions on their potential willingness to engage with location-aware technologies as a form of authorisation. User's general attitudes to using mobiles and tablets for online services such as shopping and ecommerce transactions were gathered.

Tablets and mobile devices are both used to access banking and shopping applications. A large proportion (86.11%) of users' access banking services and online shopping from home via tablet devices. Although 70% of respondents reported using banking services anywhere. There was still significant usage across different locations (Home, Work, College etc.) to justify the use of location-based authorisation.

Users were then asked about their views on whether location should be used for restricting transactions. Whilst some respondents did not think transactions should be restricted at all the majority of users agreed that if restrictions using location were introduced then this should only be done if they could customise controls on how it affects them.

A sample application was designed to demonstrate how location-based authorisation might work. The design was influenced by the initial survey with many common phone based controls. The concept of using location this way also relates to the LRBAC model within section 2.3.5 of this document. The application was positioned as an extension of a banking application. A second smaller focus group was recruited from the initial survey set in order to gauge opinions on the application. The focus group were shown iPhone layouts and then asked to feedback whether they would consider using the application if their bank offered it to them. The feedback took place in the form of an additional online survey.

The results showed significant interest in using location-based authorisation but only if it was within their banking applications. The security offered by this approach outweighed the privacy concerns the users may have. This demonstrates and justifies the need to develop an application framework to support location-based authorisation.

8.1 Review of Objectives

The first objective is section 1.3.2 was to provide a thorough review of how location is determined on a smartphone and the enabling technologies. Section 2.3 provides a detailed review of the main technologies that provide the main location enabling technologies. Position data has improved with the advancement from GPS to A-GPS and even using known locations of access points to help weak signal areas still provide positioning data to mobile devices.

A-GPS overcame the hardware demands of GPS location positioning by removing the need for technology in the device and instead placing that technology into cell tower location servers. The issue of GPS indoors and in areas where insufficient GPS satellite positions can be seen was reduced with the approach taken in wireless fingerprinting.

The second objective was to investigate the state of the art in using smartphone location as a means to authorise mobile services. Section 2.5 shows that the banking sector is looking at using location as a means of authorisation within ATM machines. In a similar vein using location as a means of authorisation for payment systems in checking the purchaser's mobile is in the vicinity of the store is being considered. Amazon are also looking at proximity verification for sending payments via smartphones to different users. The challenge with the approaches taken is the varying rules that may take place if for example the mobile battery dies. However, there is clear indication that using location as an additional means of authorisation security can strengthen user protection from mobile fraud. Many of the existing security systems still rely on a single point of access i.e. password.

In July, 2014 Apple Inc published a patent (Apple, 2014) for location-sensitive security levels and setting profiles based on detected location. The patent shows how Apple plan to allow iPhone applications to bypass the lock screen based on location. Figure 25 shows similar location settings to the sample application in this research. Apple's controls appear to be focused around different security levels for the device depending on location. The example shows the ability for users to define a location as mobile or fixed.

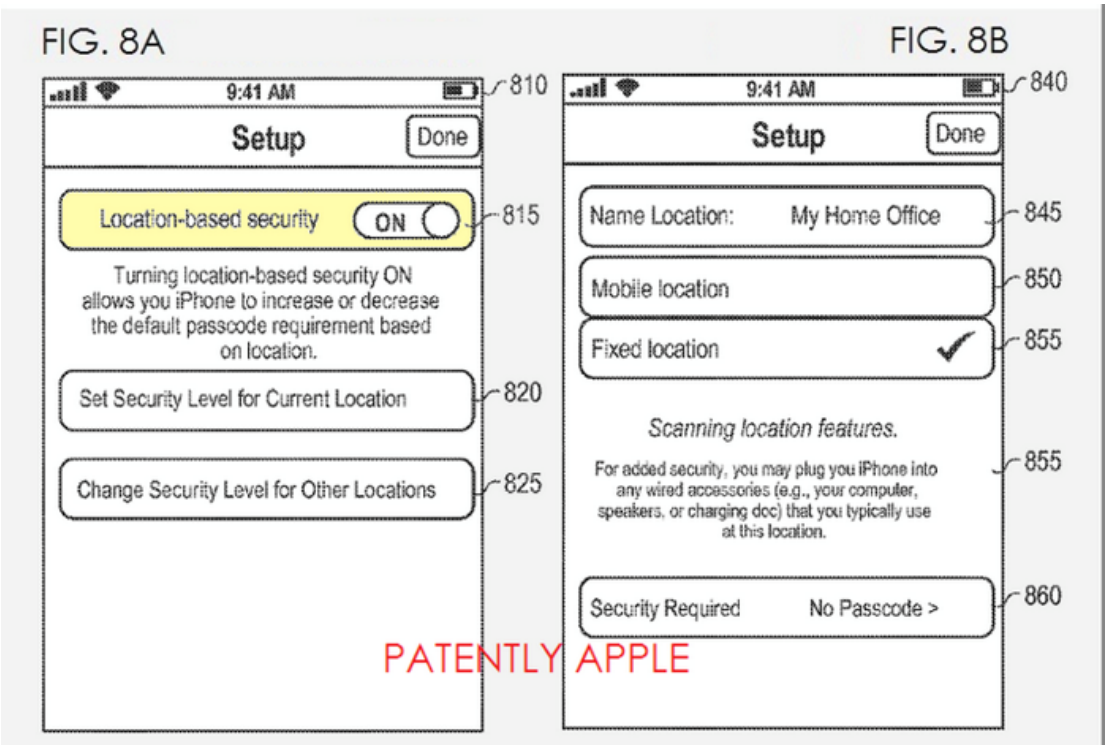


Figure 25. Location Setting Controls (Apple, 2014)

Once the location has been defined rules can be setup for passcodes and iPhone actions as shown in Figure 26. If a leading company like Apple plan to include location controls in a future release of their iOS then it is probable that users will gain more familiarity with using location as a means of security. This development adds more justification to the designs in this research.

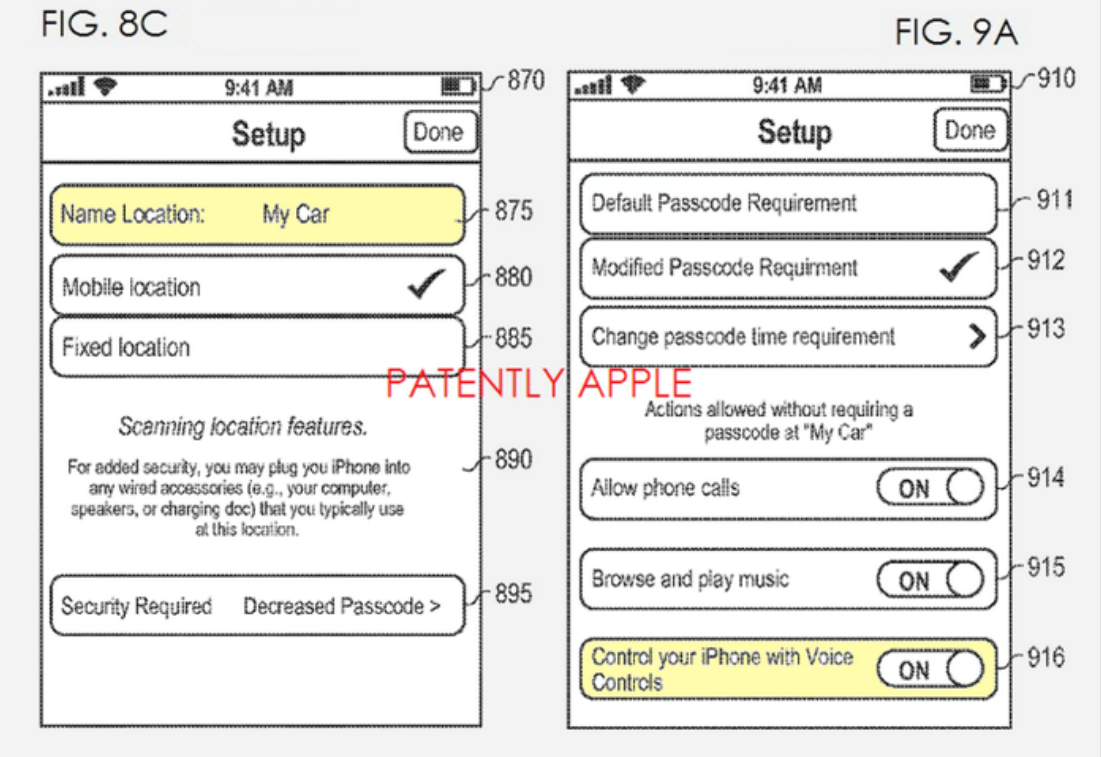


Figure 26. Apple's passcode and action setup screens (Apple, 2014).

The third objective was to identify any current limitations and issues with using location as a means of authorisation. Section 2.3 identified challenges to location services. Clearly there are potential attack vectors that enable hackers to gain or alter device location. GPS Spoofing, replay attacks, jamming have created significant risks to the shipping sector. These attack vectors lead to the introduction of the eLORAN system detailed in section 2.4.4. The eLORAN system offers a secondary check of location data to ensure no spoofing etc. is taking place. Section 2.4.8 outlines a similar system but using the GPS military encrypted signal as a means of comparison across a number of satellites. Clearly these frameworks could be used to reduce the potential attack vectors on the location based authorisation application presented in this thesis. It is important to note that whilst there is a potential risk against the proposed system the location is not the entirety of the security for the user. It is an additional means of authorising transactions. Deploying location based authorisation in this way would make the challenge of hackers more difficult and timely which may lead them to reduce their attacks to users of this type of system.

The fourth objective was to design and develop a user study to investigate the user willingness to use location to authorise mobile services. An online survey was designed to understand users' general use of mobiles and tablets. Users were asked about their general understanding of location technology and their opinions of whether restricting transactions with location was something they would use. The survey results supported the use of location as a means to authorise transactions. However, it was clear from the initial survey that users would only engage with this approach if they had sufficient user controls to customise the security. This lead to the designs shown in Chapter 5. A smaller focus group were shown the designs and there was significant support for the application. Users even agreed that the potential benefits of the protections offered outweighed any privacy concerns they had. The trust would deteriorate if the application was outside of a banking application although placing the application within the Verified by Visa layer may be beneficial if the controls could remain within the banking application.

8.2 Research Questions Answered

Section 1.3.1 lists the following research questions, which have been used in this thesis to drive the research objectives and hypothesis of the thesis. This section concludes each of the research questions in relation to research carried out.

Can location-aware technologies be used in financial environments to reduce users' exposure to fraud?

This research demonstrates how location-aware technologies could be used to reduce users exposure to fraud. GPS or A-GPS can be used to verify location of the mobile device and compare to the user defined geo-mapped area as shown in the sample application in Figure 23. There are also models in existence such as location-aware role based access control (LRBAC) described in section 2.3.5 that could be applied to the application designed in this thesis.

There are potential attack vectors such as GPS spoofing but there are countermeasures to verify GPS location that could still be deployed as shown in the literature review in chapter 2. The challenge is still that the countermeasures do not yet appear to be available to the average consumers smart-phone. The use of location-aware transactions is suggested here as an additional line of defence rather than any suggestion that it is offered as a complete solution.

Are users willing to consider the use of location-aware technologies linked to financial services as a mechanism for reducing fraud?

This research question was tested via the use of a survey of user experiences in relation to m-Commerce via mobile devices. First, a number of user acceptance frameworks were reviewed in order to help create 9 hypothesise. Each hypothesis was used to create the survey questions in chapter 3 and also in the application design survey in chapter 5. The results showed that users are willing to engage with location-aware technologies as a mechanism to reduce fraud. The initial survey demonstrated that users only support this approach if sufficient user controls were enabled. They were also clear that they would trust an application less if it were not based within their banks application. This led to the design of the example application in chapter 5. The second survey then resulted in 90% of respondents stating that they were willing to use a system like this as a mechanism to reduce fraud.

What are the challenges involved in linking location-aware services to realise a solution, which meets user needs whilst providing an extra layer of security for financial transactions?

This research demonstrates that there are challenges in relation to the attack vectors against using location. GPS spoofing can be deployed to mimic a known location such as a users home address. Clearly, mainstream counter measures need to be deployed such as geoencryption detailed in section 2.4.7 to further strengthen this suggested approach of securing m-Commerce transactions using location. The challenge is deploying countermeasures in a

relatively easy form that users can understand or consider the effort expectancy sufficient to be worth them engaging with.

The issue of privacy seems to be less of a concern as long as the application is within the users banking application. Users reported that the benefits outweighed the privacy concerns when shown the sample application.

There is also the challenge of delivering a real application based on this research. The next stage would require a banking and/or Visa/Mastercard partner to discuss the implementation of a pilot application. The underpinning query time required at the point of placing a transaction may be problematic. For example, checking and verifying user current location against stored database values may cause issues in terms of performance and also user experience. This issue is beyond the scope of this research document and would require separate research.

There appears to be a fine balance between delivering a system secure enough to protect consumers but simple enough for them to both understand and engage with.

8.3 Reflections

There was a significant survey population that did not presently use their mobiles for banking or shopping online (41.19% do not access mobile banking and 54.61% did not use their mobile device for online shopping). It would have been beneficial to include some of this population in the second survey after showing the example banking application. This would have provided an insight whether the security offered would make them consider using mobiles for banking or shopping online.

There is an assumption in the design of the example application that devices can be easily identified by installing a certificate on the device. This assumption has been made without a full understanding of how location-based queries could be carried out within banking database systems.

The example application was based on the iPhone framework but clearly a deployed application would need to be cross platform covering other devices such as Android or Blackberry.

The survey data for the second survey was significantly lower than the initial survey (20 as opposed to 116). The second survey population may have been made up of technology keen early adopters. This could further affect the positive acceptance of the application.

The outcome of both the surveys could be different if a larger population sample was used. 116 respondents is still a small sample against the population of users who may be using smart-phones and tablets.

8.4 Future Work

The example application showed device management controls. These were based on the concept of certificate deployment. More research is required to understand the use of certificates this way to identify if they can be used to verify device identity and protect against identity fraud.

This research should be discussed with both the banking sector and Visa/MasterCard to gain an understanding of where an application like this would be placed in terms of data locations. It may be that the application sits in the banks current application but calls are allowed from Visa/MasterCard to verify transactions or services. There is a clear need for a banking research partner to develop this application further.

An understanding of how banks use metadata to verify identity will be required in order to understand issues like query load time to ensure that the location-based metadata from the location-based application works at the time of transactions checking. For example, how long would it take the verified by visa screen shown in Figure 24 to verify the users or device location in order to approve or deny the transaction.

A detailed evaluation of the payment process of online shopping platforms is required to understand the best way of identifying the origin of payment requests so that the location-based authorisation can take place effectively.

Additionally, research into the certificate management within the context of device management and checking is required to ensure that this is the most appropriate and secure way of identifying devices and verifying their identity.

8.5 Summary

This research has demonstrated that location-aware technologies can be used in a financial environment to reduce a user's exposure to fraud. It also provides evidence of user willingness to engage with location-based authorisation applications as long as there are sufficient controls and that the application forms part of their current banking application.

Reference List

Aittola, Markus, Tapio Ryhanen, and Timo Ojala. 2003. SmartLibrary - Location-Aware Mobile Library Service. *Human-Computer Interaction with Mobile Devices and Services (2003)*. **2795**, pp.411-416.

Aloul, F, A Sagahyroon, A Al-Shami et al. 2009. Using mobiles for on campus location tracking. *In*: *MoMM '09 Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia*. Kuala Lumpur: ACM, pp.231-235.

Anwar, Al Kateeb, Gragopoulos Ioannis, and F N Pavlidou. 2008. Evaluation of indoor Location Based on combination of AGPS / HSGPS. *In*: *Wireless Pervasive Computing, 2008. ISWPC 2008. 3rd International Symposium on*. Santorini: IEEE, pp.383-387.

Apple. 2014. *Location-Sensitive Security Levels and Setting Profiles based on detected location*. US2014/0187200 A1.

Becker, Georg T, Sherman C Lo, David S De Lorenzo et al. 2010. Secure location verification: a security analysis of GPS signal authentication. *In*: Sara Foresti and Sushil Jajodia, (eds). *DBSec'10 Proceedings of the 24th annual IFIP WG 11.3 working conference on Data and applications security and privacy*. Berlin: Springer-Verlag, pp.366-373.

Block, James, Thomas H Graef, Natarajan Ramachandran et al. 2013. *ATM transaction authorization based on user location verification*. 8459546.

Burrell, Gay K. 2001. Collectively defining context in a mobile, networked computing environment. *Proceedings of the Conference on Human Factors in Computing Systems, Association for Computing Machinery*., pp.231-232.

Caruso and Salaway, Gail. 2008. *Educause Center for Applied Research*. [online]. [Accessed 10 October 2011]. Available from World Wide Web: <://www.harford.edu/technology/TAC/Meetings/2008-11-17/ECARRoadmap_Students2008.pdf>

Cavaleri, Antonio, Beatrice Motella, Marco Pini, and Maurizio Fantino. 2010. Detection of Spoofed GPS Signals at Code and Carrier Tracking Level. *In*: *5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*. Noordwijk: IEEE, pp.1-6.

Chen, Guanling and David Kotz. 2000. *A Survey of Context-Aware Mobile Computing Research*. Hanover: Dartmouth College.

Davis, Fred D. 1989. Perceieved Usefulness, Percieved Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*. **13**(3), pp.319-340.

Diwakar , Gupta, Paul C Schattauer, Chih-Jen Huang, and Kiran Kumar Meduri. 2013. *Location aware transaction authorization*. US8509734 B1.

El-Bakry, Hazem M and Nikos Mastorakis. 2009. Design of Anti-GPS for Reasons of Security. *RECENT ADVANCES IN APPLIED MATHEMATICS AND COMPUTATIONAL AND INFORMATION SCIENCES*. **2**, pp.480-500.

Federal Communciations Commission. *Wireless 911 Services*. [online]. [Accessed 13 Nov 2011]. Available from World Wide Web: <://www.fcc.gov/guides/wireless-911-services>

Feng, Shaojun and Choi Look Law. 2002. Assisted GPS and Its Impact on Navigation in Intelligent Transportation Systems. *In*: *The IEEE 5th International Conference on Intelligent Transportation Systems*. Singapore: IEEE, pp.926-931.

Finkenzeller, Klaus. 2010. *RFID Handbook: Fundamentals and Applicatons in Contactless Smart cards, Radio Frequency Identification and near-field communication (Kindle Edition]*. Chichester: John Wiley & Sons, Ltd.

Garrido, Pilar Castro, Guillermo Matas Miraz, Irene Luque Ruiz, and Miguel Ángel Gómez-Nieto. 2010. A Near Field Communication Tool for Building Intelligent Environment using Smart Posters. *INTERNATIONAL JOURNAL OF COMPUTERS AND COMMUNICATIONS*. **4**(1), pp.1-8.

Gartner , Inc. 2011. *Gartner Newsroom*. [online]. [Accessed 11 October 2011]. Available from World Wide Web: <://www.gartner.com/it/page.jsp?id=1543014>

GDAL. 2011. *GDAL - Geospatial Data Abstraction Library*. [online]. [Accessed 10 Jan 2012]. Available from World Wide Web: <://www.gdal.org/index.html>

Grant, Alan. 2008. *GPS Jamming Trial*. International Loran Association.

Grigg, M David, Matthew A Calman , Marc Warshawsky, and Raja Bose. 2013. *FRAUD PROTECTION WITH USER LOCATION VERIFICATION*. 13/213696.

Hahn, Jim and Alaina Morales. 2011. Rapid Prototyping a Collections-based Mobile Wayfinding Application. *The Journal of Academic Librarianship*. **37**(5), pp.416-422.

Head, Alison J and Michael B Eisenberg. 2010. *PROJECT INFORMATION LITERACY PROGRESS REPORT*. Washington.

Hewlett PackardHP Laboratories Palo Alto. 2006. Authorization-Based Access Control for the Services Oriented Architecture. *In*: H Alan Karp, (ed). *Fourth International Conference on Creating, Connecting, and Collaborating through Computing*. Berkeley: HP, pp.26-27.

Huang, Jiung-yao , Sheng-Yuan Huang, Po-Chun Lin et al. 2009. CampusGenie – A Campus-life Assistant on the Mobile-phone. *In*: *PCM '09 Proceedings of the 10th Pacific Rim Conference on Multimedia: Advances in Multimedia Information Processing*. Berlin: Springer-Verlag, pp.1086 - 1092.

International Loran Association. 2007. *Enhanced Loran (eLoran) Definition Document*. International Loran Association.

Ishaya, Tanko. 2012. *Business Intelligence Through Personalised Location-Aware Service Delivery*. [online]. [Accessed 1 Apr 2012]. Available from World Wide Web: <://www.intechopen.com/books/howtoreference/advances-in-customer-relationship-management/business-intelligence-through-personalised-location-aware-service-delivery>

Kannhavong, B, H Nakayama, Y Nemoto, and N Kato. 2007. A survey of routing attacks in mobile ad hoc networks. *Wireless Communications*. **14**(5), pp.85-91.

Karimi, Rohollah and Mohammad Kalantari. 2011. Enhancing Security and Confidentiality on Mobile Devices by Location-based Data Encryption. *In*: *17th IEEE International Conference on Networks (ICON)*. Singapore: IEEE, pp.241-245.

Karp, Alan H, Harry Haury, and H Michael Davis. 2009. *From ABAC to ZBAC: The Evolution of Access Control Models*. HP Laboratories HP Labs Technical Report HPL-2009-30.

Kaspersky Labs. 2013. *Apple of Discord*. [online]. [Accessed 24 Oct 2013]. Available from World Wide Web: < ://www.securelist.com/en/blog/8108/Apple_of_discord>

Keenan, Peter. 2013. *Zapp News*. [online]. [Accessed 23 Jan 2014]. Available from World Wide Web: < ://d28hiyxl50ptna.cloudfront.net/presentations/mobile-payments-a-frontier-for-innovation.pdf>

Korhonen, J, T Ojala, M Klemola, and Pasi Vaananen. 2006. mTag - Architecture for Discovering Location Specific Mobile Web Services Using RFID and Its Evaluation with Two Case Studies. *In*: *Advanced International Conference on Telecommunications / Internet and Web Applications and Services, International Conference on*. Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services (AICT-ICIW'06), p.191.

Krishnamoorthy, Shivsubramani and Ashok Agrawala. 2011. Poster: a context-aware framework for mobile applications. *In*: *MobiSys '11 Proceedings of the 9th international conference on Mobile systems, applications, and services*. New York: ACM, p.403.

Kuseler, T and I A Kami. 2012. Using Geographical Location as an Authentication Factor to Enhance mCommerce Applications on Smartphones.. *Internation Journal of Computer Science and Security*. **6**(4), pp.277-287.

Lee, Hyangjin and Jeeyeon Kim. 2006. Privacy threats and issues in mobile RFID. *In*: *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on*. IEEE, p.5.

Leon, Pedro Giovanni, Blase Ur, Yang Wang et al. What matters to users?: factors that affect users' willingness to share information with online advertisers. *In*: *SOUPS '13 Proceedings of the Ninth Symposium on Usable Privacy and Security*. New York: ACM, pp.1-19.

Lime Survey. 2012. *Features*. [online]. [Accessed 12 Mar 2012]. Available from World Wide Web: <://www.limesurvey.org/en/about-limesurvey/features>

Lionel, Ni M , Yunhao Liu, Yiu Cho Lau, and Abhishek P Patil. 2004. LANDMARC: Indoor Location Sensing Using Active RFID. *Wireless Networks*. **10**(6), pp.701-710.

Loke, W Seng. 2010. Incremental awareness and compositionality: A design philosophy for context-aware pervasive systems. *Pervasive and Mobile Computing*. **6**(2), pp.239-253.

Lu, Chris, Maiga Chang, Dr Kinshuk et al. 2011. Usability of Context-Aware Mobile Educational Game. *Knowledge Management & E-Learning: An International Journal (KM&EL)*. **3**(3).

Luo, Wanying and Urs Hengartner. 2010. Proving your location without giving up your privacy. *In*: *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*. New York: ACM, pp.7-12.

Microsoft Corporation. 2013. *Microsoft Security Intelligence Report*. [online]. [Accessed 31 Oct 2013]. Available from World Wide Web: <://www.microsoft.com/security/sir/default.aspx>

mobiThinking. 2013. *Global mobile statistics 2013 Part A: Mobile subscribers; handset market share; mobile operators*. [online]. [Accessed 5 Oct 2013]. Available from World Wide Web: <://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#subscribers>

Moore, A Geoffrey. 1991. *Crossing the Chasm*. HarperCollins.

Oasis. 2009. *Devices Profile for Web Services (DPWS)*. [online]. [Accessed 30 Sep 2013]. Available from World Wide Web: <://docs.oasis-open.org/ws-dd/ns/dpws/2009/01>

Paterson, Lorraine and Boon Low. 2011. Student attitudes towards mobile Libary services for smartphones. *Library Hi Tech*. **29**(3), pp.412-423.

Popescu. 2010. *Geolocation API Specification*. [online]. [Accessed 13 Nov 2011]. Available from World Wide Web: <://dev.w3.org/geo/api/spec-source.html>

Price Waterhouse Coopers. 2011. *AML Topics*. [online]. [Accessed 25 Jan 2014]. Available from World Wide Web: <://www.pwc.com/us/en/anti-money-laundering/publications/assets/aml-transaction-monitoring-improvement.pdf>

Qiu, Di, Sherman Lo, and Per Enge. 2007. Geoencryption with Loran. *In*: *Proceedings of International Loran Association*. Stanford: Stanford University, pp.1-9.

Ray, Indrakshi, Mahendra Kumar, and Lijun Yu. 2006. *Information Systems Security*. Berlin: Springer.

Robson, Colin. 2002. *Real World Research*. Oxford: Blackwell Publishing.

Roman, P and C Bergholtz. 2012. *Mobile Commerce from Evolution to revolution*. [online]. [Accessed 30 Sep 2013]. Available from World Wide Web: <://www.twinklemagazine.nl/achtergronden/2012/09/rapport-bedrijven-laten-mogelijkheden-m-commerce-liggen/GP-Bullhound-Research-Mobile-Commerce-September-2012.pdf>

Rouillard, José. 2008. Contextual QR Codes. *In*: *The Third International Multi-Conference on Computing in the Global Information Technology*. Athens: IEEE, pp.50 - 55.

Sandhu, Ravi S and Pierangela Samarati. 1994. Access Contol: Principles and Practice. *IEE Communications Magazine*. **32**(9), pp.40-48.

Schilit, B N and M M Theimer. 2002. Disseminating active map information to mobile hosts. *Network*. **8**(5), pp.22-32.

Sharma, Meenakshi. 2010. RFID Based Mobiles: Next Generation Applications. *In*: *Information Management and Engineering (ICIME), 2010 The 2nd IEEE International Conference on*. IEEE, pp.523-526.

Skyhook Wireless. 2011. *Skyhook How it Works*. [online]. [Accessed 13 Nov 2011]. Available from World Wide Web: <://www.skyhookwireless.com/howitworks/>

Stephens, Ryan L. 2010. *Mobile Application Security and User Trust*. [online]. [Accessed 2 Jan 2014]. Available from World Wide Web: <://www.adaptivesoftwareconcepts.com/wp-content/uploads/2013/08/Mobile-Application-Security-and-User-Trust.pdf>

Straub, Evan T. 2009. Understanding Technology Adoption: Theory and Future Directions for Informal Learning. *Review of Education Research*. **79**(2), pp.625-649.

U.S. Goverment. 2011. *GPS.gov*. [online]. [Accessed 15 October 2011]. Available from World Wide Web: <://www.gps.gov/systems/gps/>

U.S. Goverment. 2013. *GPS.gov*. [online]. [Accessed 28 September 2013]. Available from World Wide Web: <://www.gps.gov>

US Department of Commerce. 1992. Role-Based Access Controls. *In*: David F Ferraiolo and D Richard Kuhn, (eds). *15th National Computer Security Conference*. Baltimore: National Institute of Standards and Technology, pp.554-563.

Van Diggelen, Frank. 2009. *A-GPS: Assisted GPS, GNSS, and SBAS*. London: Artech House.

Venkatesh , Viswanath, James Y. L Thong, and Xin Xu. 2012. CONSUMER ACCEPTANCE AND USE OF INFORMATION TECHNOLOGY: EXTENDING THE UNIFIED THEORY OF ACCEPTANCE AND USE OF TECHNOLOGY. *MIS Quarterly*. **36**(1), pp.157-178.

Venkatesh, Viswanath, Michael G Morris, Fred D Davis, and Gordon B Davis. 2003. USER ACCEPTANCE OF INFORMATION TECHNOLOGY: TOWARD A UNIFIED VIEW. *MIS Quarterly*. **27**(3), pp.425-478.

Visa Europe Ltd. 2014. *Verified by Visa*. [online]. [Accessed 02 Aug 2014]. Available from World Wide Web: <://www.visaeurope.com/en/cardholders/verified_by_visa.aspx>

Wang, Jingguo, Tejaswini Herath, Rui Chen et al. 2012. Research Article Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email. *IEEE TRANSACTIONS ON PROFESSIONAL COMMUNICATION*. **55**(4), pp.345-362.

Warner, Jon S and Roger G Johnston. 2002. A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing. *The Journal of Security Adminsitration*. **25**, pp.19-28.

Wen, Hengqing, Huang Yih-Ru, John Dyer et al. 2005. Counter Measures for GPS signal spoofing. *Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2005)*., pp.1285-1290.

Worldpay. 2012. *Are you giving your customers what they really, really want?* [online]. [Accessed 1 Jan 2013]. Available from World Wide Web: <://worldpay.co.uk/media/index.php?page=archive⊂=retail-report&c=>

Xu, Heng, Xin Luo, John Carroll, and Mary Beth Rosson. 2010. The personalization privacy paradox: An exploratory study of decision making

process for location-aware marketing. *Descision Support Systems*. **51**(1), pp.42-52.

Zandbergen, P A. 2009. Accuracy of iPhone Locations: A Comparison of Assisted GPS, WiFi, and Cellular Positioning. *Transactions in GIS*. **13**(s1), pp.5-25.

Zaragoza. 2013. *Spoofing a Superyacht at Sea*. [online]. [Accessed 10 Nov 2013]. Available from World Wide Web: <://www.utexas.edu/know/2013/07/30/spoofing-a-superyacht-at-sea/>

Zhang, Dongsong, Boonlit Adipat, and Yaser Mowafi. 2009. User-Centered Context-Aware Mobile Applications—The Next Generation of Personal Mobile Computing. *Communications of the Association for Information Systems*. **24**(3), pp.28-46.

Zhou, Tao. 2011. An empirical examination of initial trust in mobile banking. *Internet Research*. **21**(5), pp.527-540.

Zhou, Tao, Yaobin Lu, and Bin Wang. 2010. Integrating TTF and UTAUT to explain mobile banking user adoption. *Computers in Human Behaviour*. **26**(4), pp.760-767.

Appendices

Appendix A – Pilot Survey Version 1

Section 1 Basic Information

This section relates to background information about your gender, age, education.

1 [Gender] Please select your gender.

Please choose that apply:

- Male
- Female

2) Please select your age.

Please choose that apply:

- Under 21
- 21-25
- 26-30
- 31-35
- 36-40
- 41-45
- 46-50
- 50+

3) [Education] Please Select Your Highest Education Level

- GSCE/O Levels
- A-Levels
- BTEC
- Foundation Degree
- Degree BA/BSc
- Masters Degree Msc/MA
- PHD

Current Job

4) Please state your current occupation _____

Section 2 Approaches to technology

This section relates to your attitudes to technology specifically mobile devices.

Mobile Phone Details

5) Current Mobile Make and Model _____

6) Do you use your phone for the following Applications/Services:-

- Mobile Banking
- Ebay purchases
- Amazon Purchases
- Online shopping
- Game Apps
- Social Networking Apps
- Foursquare
- Sat Nav Applications
- Maps

Tablet Details

7) Do you own a tablet device?

7a) If yes what make and model?

7b) Does your tablet have a SIM installed to enable you to use it away from a WIFI connection?

8) Do you use your Tablet for the following Applications/Services:-

- Mobile Banking
- Ebay purchases
- Amazon Purchases
- Online shopping
- Game Apps

- Social Networking Apps
- Foursquare
- Sat Nav Applications
- Maps

Your attitudes to technology:-

Please state how much you agree or disagree with the following questions.

Strongly Agree ☐ Agree ☐ Neither Agree or Disagree ☐ Disagree ☐ Strongly Disagree ☐

9) When new mobile devices are released I make sure I purchase or upgrade as soon as possible.

10) I feel technology is a central part of my life.

11) When new mobiles and tablets are released I find it easy to understand the benefits of using the new devices.

12) When new mobiles and tablets are released I often feel they are passing fads and prefer to wait and see how others use them before making a decision to use myself.

13) When new mobiles and tablets are released I worry about my ability to utilise the new functions so wait until there is more help and support available.

14) I have no interest in using the latest mobile and tablets.

Mobile Commerce

Mobile commerce sometimes referred to as m-commerce refers to online transactions carried out by portable devices such as mobiles and tablets. This could be online banking, shopping online etc. This section relates to any transactions you may do with your mobile devices and tablets.

15) How often do you access your bank account via your mobile or tablet?

- Once a day

- More than once a day
- once a week
- never
- other

16) What activities do you carry out with your banking application on your devices?

- Balance Enquiry
- Bill Payment
- Statement Enquiry

17) Where do you access your online banking facilities?

- Only at home
- Only at work/university,
- both home and work,
- on the way to and from work,
- Anywhere.
- Other _____

18) Have you ever been victim to financial fraud? i.e. Card access, online access to bank or purchases without your consent? YES/NO

18a) If yes please state the type of fraud with any details you are comfortable to share.

A Phishing attack is where a criminal pretends to be from an organisation they are not from such as your bank or auction site and they usually provide a link for you to verify your account details. The victim then has their login details to the legitimate service stolen and used to defraud the victim further.

19) Have you ever been a victim of a Phishing attack?

19a) If yes was that via an email received on a mobile device? If so please provide basic details.

Please state how much you agree or disagree with the following statement:-

20) Accessing online banking and shopping is more secure on my desktop pc than a mobile or tablet.

Strongly Agree ☐ Agree ☐ Neither Agree or Disagree ☐ Disagree ☐

Strongly Disagree ☐

Location-aware Services

Your mobile phone and tablet can access GPS services to provide you and application providers with your current location. This can often lead to more relevant information being sent to you such as offers in shops in your vicinity or check – in services that exist in social networking sites such as Facebook or Foursquare and also Twitter. You can often control these settings in your phones settings menu.

21) Are you aware of location services on mobile and tablet devices?

22) Do you use any applications that use your device location?

22a) If so what?

Please state how much you agree or disagree with the following statements.

23) I find location services to complex to use.

Strongly Agree ☐ Agree ☐ Neither Agree or Disagree ☐ Disagree ☐

Strongly Disagree ☐

24) I am concerned about my privacy too much to consider using location services on mobile or tablet devices.

Strongly Agree ☐ Agree ☐ Neither Agree or Disagree ☐ Disagree ☐

Strongly Disagree ☐

25) Do you know how to customise location settings for mobile or tablet devices?

25a) If so, do you customise location settings for any applications that you are aware use the information?

26) Why?

This research looks at the concept of you being able to decide where your device can carry out mobile transactions to reduce the possibility of mobile fraud. An example would be the ability to only enable bank statements access when at work or home locations. You may then decide that you will allow your devices to buy products and services in particular areas where you live. The idea is that even if someone managed to gain access to your login details they would have to be physically in your predefined are in order to carry out that transaction.

After considering this statement please state how much you agree or disagree with the following statements.

Strongly Agree ☐ Agree ☐ Neither Agree or Disagree ☐ Disagree ☐

Strongly Disagree ☐

27) Mobile devices and tablets should not be restricted by location at all.

28) The ability to use device location within your banks mobile application to authorise different levels of access would make me trust the security of the application more.

29) If the bank stored my location data I would be less inclined to use it.

30) Restricting where I can buy products and services on a mobile device or tablet would be too restrictive.

31) The ability to use location as a means to authorise mobile transactions would provide me with a better protection against fraud.

31a) Any other comments?

There will be a smaller further survey to show some visual examples of how proposed applications would work.

Appendix B – Pilot Survey 2

This survey forms part of my Post Graduate Research into whether people are willing to use smart-phone location-aware services to secure mobile and tablet transactions. It is exploring a system where by you could decide what geographic locations you allow a tablet or mobile to carry out different transactions. For example you may want to allow banking access when at home locations or work but not anywhere else. The purpose of the system is to help protect mobile users from fraud.

No personal identifiable data will be stored with survey results.

Section 1 Basic Information

This section relates to background information about your gender, age, education.

1 [Gender] Please select your gender.

Please choose that apply:

- Male
- Female

2) Please select your age.

Please choose that apply:

- Under 21
- 21-25
- 26-30
- 31-35
- 36-40
- 41-45
- 46-50
- 50+

3) [Education] Please Select Your Highest Education Level

- GSCE/O Levels
- A-Levels
- BTEC
- Foundation Degree
- Degree BA/BSc
- Masters Degree Msc/MA
- PHD

Current Job

4) Please state your current occupation _____

Section 2 Approaches to technology

This section relates to your attitudes to technology specifically mobile devices.

Mobile Phone Details

5) Current Mobile Make and Model _____

6) Do you use your phone for the following Applications/Services:-

- Mobile Banking
- Ebay purchases
- Amazon Purchases
- Online shopping
- Game Apps
- Social Networking Apps
- Foursquare
- Sat Nav Applications
- Maps

Tablet Details

7) Do you own a tablet device?

7a) If yes what make and model?

7b) Does your tablet have a SIM installed to enable you to use it away from a WIFI connection?

8) Do you use your Tablet for the following Applications/Services:-

- Mobile Banking
- Ebay purchases
- Amazon Purchases
- Online shopping
- Game Apps
- Social Networking Apps
- Foursquare
- Sat Nav Applications
- Maps

Your attitudes to technology:-

Please state how much you agree or disagree with the following questions.

Strongly Agree ☐ Agree ☐ Neither Agree or Disagree ☐ Disagree ☐ Strongly Disagree ☐

9) When new mobile devices are released I make sure I purchase or upgrade as soon as possible.

10) I feel technology is a central part of my life.

11) When new mobiles and tablets are released I find it easy to understand the benefits of using the new devices.

12) When new mobiles and tablets are released I often feel they are passing fads and prefer to wait and see how others use them before making a decision to use myself.

13) When new mobiles and tablets are released I worry about my ability to utilise the new functions so wait until there is more help and support available.

14) I have no interest in using the latest mobile and tablets.

Mobile Commerce

Mobile commerce sometimes referred to as m-commerce refers to online transactions carried out by portable devices such as mobiles and tablets. This could be online banking, shopping online etc. This section relates to any transactions you may do with your mobile devices and tablets.

15) How often do you access your bank account via your mobile?

- Once a day
- More than once a day
- once a week
- other

15b) How often do you access your bank account via your tablet?

- Once a day
- More than once a day
- once a week
- other

16) What activities do you carry out (on your mobile device) with your banking application on your devices?

- Balance Enquiry
- Bill Payment
- Statement Enquiry
- Other (State)

16b) What activities do you carry out (on your tablet device) with your banking application on your devices?

- Balance Enquiry
- Bill Payment
- Statement Enquiry
- Other (State)

17) Where do you access your online banking facilities?

- At home
- At work / University / School
- on the way to and from work,
- Anywhere.
- Other _____

18) Do you make purchases on your mobile device from online shops and services?

Yes/No

18a) If Yes, where do you make purchases from?

- Home Location
- Office Location
- College/University
- Anywhere?

19) When using your mobile device where do you make purchases from?

- At home
- At work / University / School
- on the way to and from work,
- Anywhere.
- Other _____

20) When using your tablet device where do you make purchases from?

- At home
- At work / University / School
- on the way to and from work,
- Anywhere.
- Other _____

21) Have you ever been victim to financial fraud? i.e. Card access, online access to bank or purchases without your consent? YES/NO

22) If yes please state the type of fraud with any details you are comfortable to share.

A Phishing attack is where a criminal pretends to be from an organisation they are not from such as your bank or auction site and they usually provide a link for you to verify your account details. The victim then has their login details to the legitimate service stolen and used to defraud the victim further.

23) Have you ever been a victim of a Phishing attack?

23a) If yes was that via an email received on a mobile device? If so please provide basic details.

Please state how much you agree or disagree with the following statement:-

24) Accessing online banking and shopping is more secure on my desktop pc than a mobile or tablet.

Strongly Agree ☐ Agree ☐ Neither Agree or Disagree ☐ Disagree ☐

Strongly Disagree ☐

Location-aware Services

Your mobile phone and tablet can access GPS services to provide you and application providers with your current location. This can often lead to more relevant information being sent to you such as offers in shops in your vicinity

or check – in services that exist in social networking sites such as Facebook or Foursquare and also Twitter. You can often control these settings in your phones settings menu.

25) Are you aware of location services on mobile and tablet devices?

26) Do you use any applications that use your device location on your mobile?

26a) If so what?

27) Do you use any applications that use your device location on your tablet?

28a) If so what?

Please state how much you agree or disagree with the following statements.

29) I find location services too complex to use.

Strongly Agree ☐ Agree ☐ Neither Agree or Disagree ☐ Disagree ☐

Strongly Disagree ☐

30) I am concerned about my privacy too much to consider using location services on mobile or tablet devices.

Strongly Agree ☐ Agree ☐ Neither Agree or Disagree ☐ Disagree ☐

Strongly Disagree ☐

31) Do you know how to customise location settings for mobile or tablet devices?

32) If so, do you customise location settings for any applications that you are aware use the information?

32a) Why?

This research looks at the concept of you being able to decide where your device can carry out mobile transactions to reduce the possibility of mobile

fraud. An example would be the ability to only enable bank statements access when at work or home locations. You may then decide that you will allow your devices to buy products and services in particular areas where you live. The idea is that even if someone managed to gain access to your login details they would have to be physically in your predefined area in order to carry out that transaction.

After considering this statement please state how much you agree or disagree with the following statements.

Strongly Agree ☐ Agree ☐ Neither Agree or Disagree ☐ Disagree ☐

Strongly Disagree ☐

33) Mobile devices and tablets should not be restricted by location at all.

Mobile devices and tables should only be restricted by location if I can control when and how this is setup.

I would be more interested in only restricting devices this way in the area I work and live (i.e. City/Town).

34) The ability to use device location within your banks mobile application to authorise different levels of access would make me trust the security of the application more.

35) If the bank stored my location data I would be less inclined to use it.

36) Restricting where I can buy products and services on a mobile device or tablet would be too restrictive.

37) The ability to use location as a means to authorise mobile transactions would provide me with a better protection against fraud.

37a) Any other comments?

There will be a smaller further survey to show some visual examples of how proposed applications would work. Please can you leave your email address

if and name if you are willing to engage further in a short additional survey of screen shots of a proposed system.

_____

Appendix B – Amended Survey Questionnaire

Using Mobiles and Tablets to make purchases or carry out online banking.

This survey forms part of my Post Graduate Research into whether people are willing to use smart-phone location-aware services to secure mobile and tablet transactions. It is exploring a system where by you could decide what geographic locations you allow a tablet or mobile to carry out different transactions. For example you may want to allow banking access when at home locations or work but not anywhere else. The purpose of the system is to help protect mobile users from fraud.

No personal identifiable data will be stored with survey results.

Thanks for taking part in this survey. Please leave your email address at the end of this study if you are happy to be contacted about a smaller additional survey relating to how a system would look too capture your opinions.

There are 34 questions in this survey

Basic Information

This section relates to background information about your gender age and education.

Please select your gender. *

Please choose **one** of the following:

◯ Female

◯ Male

Please select your age. *

Please choose **one** of the following:

◯ Under 21

◯ 21-30

○ 31-40

○ 41-50

○ 51-60

○ 60+

Please select your highest education level. *

Please choose **one** of the following:

○ GSCE/O Levels

○ A-Levels

○ BTEC

○ Foundation Degree

○ Degree BA/BSc

○ Masters Degree Msc/MA

○ PHD

Approaches to Technology

This section relates to your attitudes to technology specifically to mobile devices.

Please state your current make an model of of your mobile device. *

Please write your answer here:

Do you use your phone for any of the following applications/services? *

Please choose that apply:

☐ Mobile Banking

☐ Ebay Purchases

☐ Online Shopping

☐ Game Apps

☐ Social Networking Apps

☐ Foursquare

☐ Sat Nav Apps

☐ Maps

Do you own a tablet device? *

Please choose **one** of the following:

○ Yes

○ No

What is the make and model of your tablet device?

Only answer this question if the following conditions are met:
Answer was 'Yes' question '6 [ATTITUDES3]' (Do you own a tablet device?)

Please write your answer here:

Do you use your tablet for any of the following applications/services? *

Only answer this question if the following conditions are met:
Answer was 'Yes' question '6 [ATTITUDES3]' (Do you own a tablet device?)

Please choose that apply:

☐ Mobile Banking

☐ Ebay Purchases

☐ Online Shopping

☐ Game Apps

☐ Social Networking Apps

☐ Foursquare

☐ Sat Nav Apps

☐ Maps

Please state how much you agree or disagree with the following questions.

Please choose the appropriate response for each item:

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
When new mobile devices are released I make sure I purchase or upgrade as soon as possible.	○	○	○	○	○

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
I feel technology is a central part of my life.	○	○	○	○	○
When new mobiles and tablets are released I find it easy to understand the benefits of using the new devices.	○	○	○	○	○
When new mobiles and tablets are released I often feel they are passing	○	○	○	○	○

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
fads and prefer to wait and see how others use them before making a decision to use myself.					
When new mobiles and tablets are released I worry about my ability to utilise the new functions so wait until there is more help and	○	○	○	○	○

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
support available.					
I have no interest in using the latest mobile and tablets.	○	○	○	○	○

Mobile Commerce

Mobile commerce sometimes referred to as m-commerce refers to online transactions carried out by portable devices such as mobiles and tablets. This could be online banking, shopping online etc. This section relates to any transactions you may do with your mobile devices and tablets.

How often do you access your bank application via you mobile? *

Please choose that apply:

☐ Once a day

☐ More than once a day

☐ Once a week

☐ other

How often do you access your bank account on your tablet device?

Only answer this question if the following conditions are met:
Answer was question '8 [ATTITUDES5]' (Do you use your tablet for any of the following applications/services?)

Please choose that apply:

☐ Once a day

☐ More than once a day

☐ once a week

☐ other

When accessing your banking app from your mobile, what activities do you carry out?

Only answer this question if the following conditions are met:
Answer was question '5 [ATTITUDES2]' (Do you use your phone for any of the following applications/services?)

Please choose that apply:

☐ Balance Enquiry

☐ Bill Payment

☐ Statement Enquiry

☐ Other

When accessing your banking app from your tablet, what activities do you carry out?

Only answer this question if the following conditions are met:
Answer was question '8 [ATTITUDES5]' (Do you use your tablet for any of the following applications/services?)

Please choose that apply:

☐ Balance Enquiry

☐ Bill Payment

☐ Statement Enquiry

☐ Other

When using your mobile to access online banking application services, where do you access your online banking?

Only answer this question if the following conditions are met:
Answer was question '5 [ATTITUDES2]' (Do you use your phone for any of the following applications/services?)

Please choose that apply:

☐ At Home

☐ At work / University / School

☐ On the way to and from work

☐ Anywhere

☐ Other (Please state in comments)

When using your tablet to access online banking application services, where do you access your online banking?

Only answer this question if the following conditions are met:
Answer was question '8 [ATTITUDES5]' (Do you use your tablet for any of the following applications/services?)

Please choose that apply:

☐ At Home

☐ At work / University / School

☐ On the way to and from work

☐ Anywhere

☐ Other (Please state in comments)

When using your mobile device what location do you make purchases from? *

Only answer this question if the following conditions are met:
Answer was question '8 [ATTITUDES5]' (Do you use your tablet for any of the following applications/services?)

Please choose that apply:

☐ Home

☐ Work/College/University

☐ On way to and from work

☐ Anywhere

☐ Other

When using your tablet device what location do you make purchases from? *

Only answer this question if the following conditions are met:
Answer was question '8 [ATTITUDES5]' (Do you use your tablet for any of the following applications/services?)

Please choose that apply:

☐ Home

☐ Work/College/University

☐ On way to and from work

☐ Anywhere

☐ Other

Have you ever been victim to financial fraud? i.e. Card access, online access to bank or purchases without your consent? *

Please choose **one** of the following:

○ Yes

○ No

Please provide details of the type of fraud you experienced.

Only answer this question if the following conditions are met:
Answer was 'Yes' question '18 [Mcommerce9]' (Have you ever been victim to financial fraud? i.e. Card access, online access to bank or purchases without your consent?)

Please write your answer here:

Have you ever been a victim of a Phishing attack? *

Please choose **one** of the following:

○ Yes

○ No

A Phishing attack is where a criminal pretends to be from an organisation they are not from such as your bank or auction site and they usually provide a link for you to verify your account details. The victim then has their login details to the legitimate service stolen and used to defraud the victim further.

Please provide details of the phishing attack you experienced.

Only answer this question if the following conditions are met:
Answer was 'Yes' question '20 [Mcommerce11]' (Have you ever been a victim of a Phishing attack?)

Please write your answer here:

Please state how much you agree or disagree with the following statement:- *

Please choose the appropriate response for each item:

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
Accessing online banking and shopping is more secure on my desktop pc than a mobile or tablet.	○	○	○	○	○

Location-aware Services

Your mobile phone and tablet can access GPS services to provide you and application providers with your current location. This can often lead to more relevant information being sent to you such as offers in shops in your vicinity or check – in services that exist in social networking sites such as Facebook

or Foursquare and also Twitter. You can often control these settings in your device settings menu.

Are you aware of location services on mobile and tablet devices? *

Please choose **one** of the following:

◯ Yes

◯ No

Do you use any applications that use your device location on your mobile? *

Please choose **one** of the following:

◯ Yes

◯ No

Which mobile apps do you use that make use of you location?

Only answer this question if the following conditions are met: Answer was 'Yes' question '24 [location2]' (Do you use any applications that use your device location on your mobile?)

Please write your answer here:

Do you use any applications that use your device location on your tablet? *

Please choose **one** of the following:

◯ Yes

◯ No

Which tablet apps do you use that make use of you location?

Only answer this question if the following conditions are met: Answer was 'Yes' question '26 [location3]' (Do you use any applications that use your device location on your tablet?)

Please write your answer here:

Please state how much you agree or disagree with the following statements. *

Please choose the appropriate response for each item:

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
I find location services too complex to use.	○	○	○	○	○
I am concerned about my privacy too much to consider using location services on mobile	○	○	○	○	○

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
or tablet devices.					

Do you know how to customise location settings for mobile or tablet devices? *

Please choose **one** of the following:

◯ Yes

◯ No

If so, do you customise location settings for any applications that you are aware use the information? *

Only answer this question if the following conditions are met:
Answer was 'Yes' question '29 [location5]' (Do you know how to customise location settings for mobile or tablet devices?)

Please choose **one** of the following:

◯ Yes

◯ No

Why?

Only answer this question if the following conditions are met: Answer was 'Yes' 'No' question '30 [location6]' (If so, do you customise location settings for any applications that you are aware use the information?)

Please write your answer here:

Please state how much you agree or disagree with the following statements. *

Please choose the appropriate response for each item:

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
Mobile devices and tablets should not be restricted by location at all.	○	○	○	○	○
Mobile devices and tables should only be restricted by location if I can control when and how this is setup.	○	○	○	○	○
I would be more interested in only restricting devices this	○	○	○	○	○

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
way in the area I work and live (i.e. City/Town).					
The ability to use device location within your banks mobile application to authorise different levels of access would make me trust the security of the application more.	○	○	○	○	○
If the bank stored my	○	○	○	○	○

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
location data I would be less inclined to use it.					
Restricting where I can buy products and services on a mobile device or tablet would be too restrictive.	○	○	○	○	○
The ability to use location as a means to authorise mobile transactions would provide me	○	○	○	○	○

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
with a better protection against fraud.					

Further Work

This Section allows you to add additional comments and be contacted for a smaller visual survey.

Thank you for completing this survey. If you feel there is anything wrong with the questions asked or indeed anything missing please can you feedback here.

Please write your answer here:

There will be an additional visual survey after this has been completed where visual imagery of a system that would allow you to control device location security. The aim is to provide a better understanding of how a system might work and gauge you feedback. If you are happy to take part please can you leave your email address below and you will be contacted in due course.

Please write your answer here:

Submit your survey.
Thank you for completing this survey.

Appendix C – Final Survey Results

Results	
Number of records in this query:	111
Total records in survey:	111
Percentage of total:	100.00%

Browse

Field summary for BACKGROUND1 Please select your gender.		
Answer	**Count**	**Percentage**
Female (F)	48	43.24%
Male (M)	63	56.76%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for BACKGROUND2 Please select your age.		
Answer	**Count**	**Percentage**
Under 21 (A1)	0	0.00%
21-30 (A4)	54	48.65%
31-40 (A3)	29	26.13%
41-50 (A2)	20	18.02%
51-60 (A5)	7	6.31%
60+ (A6)	1	0.90%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for BACKGROUND3 Please select your highest education level.		
Answer	**Count**	**Percentage**
GSCE/O Levels (A1)	5	4.50%

Field summary for BACKGROUND3 Please select your highest education level.		
Answer	**Count**	**Percentage**
A-Levels (A2)	4	3.60%
BTEC (A3)	7	6.31%
Foundation Degree (A4)	4	3.60%
Degree BA/BSc (A5)	50	45.05%
Masters Degree Msc/MA (A6)	30	27.03%
PHD (A7)	11	9.91%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for ATTITUDES1 Please state your current make an model of of your mobile device.		
	Count	**Percentage**
Answer	111	100.00%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for ATTITUDES2 Do you use your phone for any of the following applications/services?		
Answer	**Count**	**Percentage**
Mobile Banking (SQ001)	68	61.26%
Ebay Purchases (SQ002)	51	45.95%
Online Shopping (SQ003)	64	57.66%
Game Apps (SQ004)	67	60.36%
Social Networking Apps (SQ005)	94	84.68%
Foursquare (SQ006)	9	8.11%
Sat Nav Apps (SQ007)	53	47.75%
Maps (SQ008)	94	84.68%

Field summary for ATTITUDES3 Do you own a tablet device?		
Answer	**Count**	**Percentage**
Yes (Y)	68	61.26%
No (N)	43	38.74%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for ATTITUDES4 What is the make and model of your tablet device?		
	Count	**Percentage**
Answer Browse	68	61.26%
No answer	0	0.00%
Not displayed	43	38.74%

Field summary for ATTITUDES5 Do you use your tablet for any of the following applications/services?		
Answer	**Count**	**Percentage**
Mobile Banking (SQ001)	36	32.43%
Ebay Purchases (SQ002)	36	32.43%
Online Shopping (SQ003)	47	42.34%
Game Apps (SQ004)	52	46.85%
Social Networking Apps (SQ005)	59	53.15%
Foursquare (SQ006)	3	2.70%
Sat Nav Apps (SQ007)	14	12.61%
Maps (SQ008)	46	41.44%
Not displayed	43	38.74%

Field summary for ATTITUDES6(SQ001)

Please state how much you agree or disagree with the following questions.
[When new mobile devices are released I make sure I purchase or upgrade as soon as possible.]

Answer	Count	Percentage
Strongly Agree (A1)	5	4.50%
Agree (A2)	13	11.71%
Neither Agree or Disagree (A3)	27	24.32%
Disagree (A4)	38	34.23%
Strongly Disagree (A5)	28	25.23%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for ATTITUDES6(SQ002)

Please state how much you agree or disagree with the following questions.
[I feel technology is a central part of my life.]

Answer	Count	Percentage
Strongly Agree (A1)	44	39.64%
Agree (A2)	43	38.74%
Neither Agree or Disagree (A3)	15	13.51%
Disagree (A4)	7	6.31%
Strongly Disagree (A5)	2	1.80%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for ATTITUDES6(SQ003)

Please state how much you agree or disagree with the following questions.
[When new mobiles and tablets are released I find it easy to understand the benefits of using the new devices.]

Answer	Count	Percentage
Strongly Agree (A1)	21	18.92%
Agree (A2)	45	40.54%
Neither Agree or Disagree (A3)	26	23.42%

Field summary for ATTITUDES6(SQ003)

Please state how much you agree or disagree with the following questions.
[When new mobiles and tablets are released I find it easy to understand the benefits of using the new devices.]

Answer	Count	Percentage
Disagree (A4)	15	13.51%
Strongly Disagree (A5)	4	3.60%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for ATTITUDES6(SQ004)

Please state how much you agree or disagree with the following questions.
[When new mobiles and tablets are released I often feel they are passing fads and prefer to wait and see how others use them before making a decision to use myself.]

Answer	Count	Percentage
Strongly Agree (A1)	12	10.81%
Agree (A2)	50	45.05%
Neither Agree or Disagree (A3)	29	26.13%
Disagree (A4)	15	13.51%
Strongly Disagree (A5)	5	4.50%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for ATTITUDES6(SQ005)

Please state how much you agree or disagree with the following questions.
[When new mobiles and tablets are released I worry about my ability to utilise the new functions so wait until there is more help and support available.]

Answer	Count	Percentage
Strongly Agree (A1)	1	0.90%
Agree (A2)	9	8.11%
Neither Agree or Disagree (A3)	25	22.52%
Disagree (A4)	41	36.94%

Field summary for ATTITUDES6(SQ005)

Please state how much you agree or disagree with the following questions.
[When new mobiles and tablets are released I worry about my ability to utilise the new functions so wait until there is more help and support available.]

Answer	Count	Percentage
Strongly Disagree (A5)	35	31.53%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for ATTITUDES6(SQ006)

Please state how much you agree or disagree with the following questions.
[I have no interest in using the latest mobile and tablets.]

Answer	Count	Percentage
Strongly Agree (A1)	6	5.41%
Agree (A2)	7	6.31%
Neither Agree or Disagree (A3)	31	27.93%
Disagree (A4)	36	32.43%
Strongly Disagree (A5)	31	27.93%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for Mcommerce1

How often do you access your bank application via you mobile?

Answer	Count	Percentage
Once a day (SQ001)	15	13.51%
More than once a day (SQ002)	2	1.80%
Once a week (SQ003)	37	33.33%
other (SQ005)	57	51.35%

Field summary for Mcommerce2		
How often do you access your bank account on your tablet device?		
Answer	**Count**	**Percentage**
Once a day (SQ001)	7	6.31%
More than once a day (SQ002)	0	0.00%
once a week (SQ003)	18	16.22%
other (SQ004)	11	9.91%
Not displayed	75	67.57%

Field summary for Mcommerce3		
When accessing your banking app from your mobile, what activities do you carry out?		
Answer	**Count**	**Percentage**
Balance Enquiry (SQ001)	63	56.76%
Bill Payment (SQ002)	31	27.93%
Statement Enquiry (SQ003)	32	28.83%
Other (SQ004)	11	9.91%
Not displayed	43	38.74%

Field summary for Mcommerce4		
When accessing your banking app from your tablet, what activities do you carry out?		
Answer	**Count**	**Percentage**
Balance Enquiry (SQ001)	34	30.63%
Bill Payment (SQ002)	23	20.72%
Statement Enquiry (SQ003)	21	18.92%
Other (SQ004)	4	3.60%
Not displayed	75	67.57%

Field summary for Mcommerce5		
When using your mobile to access online banking application services, where do you access your online banking?		
Answer	**Count**	**Percentage**
At Home (SQ001)	40	36.04%

Field summary for Mcommerce5		
When using your mobile to access online banking application services, where do you access your online banking?		
Answer	**Count**	**Percentage**
At work / University / School (SQ003)	33	29.73%
On the way to and from work (SQ002)	16	14.41%
Anywhere (SQ004)	48	43.24%
Other (Please state in comments) (SQ005)	0	0.00%
Not displayed	43	38.74%

Field summary for Mcommerce6		
When using your tablet to access online banking application services, where do you access your online banking?		
Answer	**Count**	**Percentage**
At Home (SQ001)	31	27.93%
At work / University / School (SQ003)	12	10.81%
On the way to and from work (SQ002)	2	1.80%
Anywhere (SQ004)	7	6.31%
Other (Please state in comments) (SQ005)	0	0.00%
Not displayed	75	67.57%

Field summary for Mcommerce7		
When using your mobile device what location do you make purchases from?		
Answer	**Count**	**Percentage**
Home (SQ001)	29	26.13%
Work/College/University (SQ002)	18	16.22%
On way to and from work (SQ003)	3	2.70%
Anywhere (SQ004)	24	21.62%
Other (SQ005)	4	3.60%

Field summary for Mcommerce7 When using your mobile device what location do you make purchases from?		
Answer	**Count**	**Percentage**
Not displayed	64	57.66%

Field summary for Mcommerce8 When using your tablet device what location do you make purchases from?		
Answer	**Count**	**Percentage**
Home (SQ001)	40	36.04%
Work/College/University (SQ002)	11	9.91%
On way to and from work (SQ003)	1	0.90%
Anywhere (SQ004)	10	9.01%
Other (SQ005)	0	0.00%
Not displayed	64	57.66%

Field summary for Mcommerce9 Have you ever been victim to financial fraud? i.e. Card access, online access to bank or purchases without your consent?		
Answer	**Count**	**Percentage**
Yes (Y)	12	10.81%
No (N)	99	89.19%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for Mcommerce10 Please provide details of the type of fraud you experienced.		
	Count	**Percentage**
Answer Browse	12	10.81%
No answer	0	0.00%
Not displayed	99	89.19%

Field summary for Mcommerce11 Have you ever been a victim of a Phishing attack?		
Answer	**Count**	**Percentage**
Yes (Y)	12	10.81%
No (N)	99	89.19%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for Mcommerce12 Please provide details of the phishing attack you experienced.		
	Count	**Percentage**
Answer Browse	11	9.91%
No answer	1	0.90%
Not displayed	99	89.19%

Field summary for Mcommerce13(SQ001) Please state how much you agree or disagree with the following statement:- [Accessing online banking and shopping is more secure on my desktop pc than a mobile or tablet.]		
Answer	**Count**	**Percentage**
Strongly Agree (A1)	12	10.81%
Agree (A2)	29	26.13%
Neither Agree or Disagree (A3)	46	41.44%
Disagree (A4)	19	17.12%
Strongly Disagree (A5)	5	4.50%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for location1

Are you aware of location services on mobile and tablet devices?

Answer	Count	Percentage
Yes (Y)	103	92.79%
No (N)	8	7.21%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for location2

Do you use any applications that use your device location on your mobile?

Answer	Count	Percentage
Yes (Y)	82	73.87%
No (N)	29	26.13%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for location2a

Which mobile apps do you use that make use of you location?

	Count	Percentage
Answer Browse	80	72.07%
No answer	2	1.80%
Not displayed	29	26.13%

Field summary for location3

Do you use any applications that use your device location on your tablet?

Answer	Count	Percentage
Yes (Y)	43	38.74%
No (N)	68	61.26%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for location3a

Which tablet apps do you use that make use of you location?

	Count	Percentage
Answer Browse	42	37.84%
No answer	1	0.90%
Not displayed	68	61.26%

Field summary for location4(SQ001)

Please state how much you agree or disagree with the following statements.
[I find location services too complex to use.]

Answer	Count	Percentage
Strongly Agree (A1)	1	0.90%
Agree (A2)	3	2.70%
Neither Agree or Disagree (A3)	37	33.33%
Disagree (A4)	43	38.74%
Strongly Disagree (A5)	27	24.32%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for location4(SQ002)

Please state how much you agree or disagree with the following statements.
[I am concerned about my privacy too much to consider using location services on mobile or tablet devices.]

Answer	Count	Percentage
Strongly Agree (A1)	10	9.01%
Agree (A2)	30	27.03%
Neither Agree or Disagree (A3)	27	24.32%
Disagree (A4)	35	31.53%
Strongly Disagree (A5)	9	8.11%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for location5 Do you know how to customise location settings for mobile or tablet devices?		
Answer	**Count**	**Percentage**
Yes (Y)	66	59.46%
No (N)	45	40.54%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for location6 If so, do you customise location settings for any applications that you are aware use the information?		
Answer	**Count**	**Percentage**
Yes (Y)	40	36.04%
No (N)	26	23.42%
No answer	0	0.00%
Not displayed	45	40.54%

Field summary for location6a Why?		
	Count	**Percentage**
Answer Browse	51	45.95%
No answer	15	13.51%
Not displayed	45	40.54%

Field summary for location7(SQ001) Please state how much you agree or disagree with the following statements. [Mobile devices and tablets should not be restricted by location at all.]		
Answer	**Count**	**Percentage**
Strongly Agree (A1)	12	10.81%

Field summary for location7(SQ001)		
Please state how much you agree or disagree with the following statements. [Mobile devices and tablets should not be restricted by location at all.]		
Answer	**Count**	**Percentage**
Agree (A2)	31	27.93%
Neither Agree or Disagree (A3)	50	45.05%
Disagree (A4)	14	12.61%
Strongly Disagree (A5)	4	3.60%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for location7(SQ007)		
Please state how much you agree or disagree with the following statements. [Mobile devices and tables should only be restricted by location if I can control when and how this is setup.]		
Answer	**Count**	**Percentage**
Strongly Agree (A1)	26	23.42%
Agree (A2)	57	51.35%
Neither Agree or Disagree (A3)	23	20.72%
Disagree (A4)	4	3.60%
Strongly Disagree (A5)	1	0.90%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for location7(SQ002)		
Please state how much you agree or disagree with the following statements. [I would be more interested in only restricting devices this way in the area I work and live (i.e. City/Town).]		
Answer	**Count**	**Percentage**
Strongly Agree (A1)	5	4.50%
Agree (A2)	34	30.63%
Neither Agree or Disagree (A3)	49	44.14%

Field summary for location7(SQ002)

Please state how much you agree or disagree with the following statements.
[I would be more interested in only restricting devices this way in the area I work and live (i.e. City/Town).]

Answer	Count	Percentage
Disagree (A4)	18	16.22%
Strongly Disagree (A5)	5	4.50%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for location7(SQ003)

Please state how much you agree or disagree with the following statements.
[The ability to use device location within your banks mobile application to authorise different levels of access would make me trust the security of the application more.]

Answer	Count	Percentage
Strongly Agree (A1)	9	8.11%
Agree (A2)	41	36.94%
Neither Agree or Disagree (A3)	40	36.04%
Disagree (A4)	15	13.51%
Strongly Disagree (A5)	6	5.41%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for location7(SQ004)

Please state how much you agree or disagree with the following statements.
[If the bank stored my location data I would be less inclined to use it.]

Answer	Count	Percentage
Strongly Agree (A1)	14	12.61%
Agree (A2)	31	27.93%
Neither Agree or Disagree (A3)	34	30.63%
Disagree (A4)	26	23.42%

Field summary for location7(SQ004) Please state how much you agree or disagree with the following statements. [If the bank stored my location data I would be less inclined to use it.]		
Answer	**Count**	**Percentage**
Strongly Disagree (A5)	6	5.41%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for location7(SQ005) Please state how much you agree or disagree with the following statements. [Restricting where I can buy products and services on a mobile device or tablet would be too restrictive.]		
Answer	**Count**	**Percentage**
Strongly Agree (A1)	23	20.72%
Agree (A2)	53	47.75%
Neither Agree or Disagree (A3)	21	18.92%
Disagree (A4)	14	12.61%
Strongly Disagree (A5)	0	0.00%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for location7(SQ006) Please state how much you agree or disagree with the following statements. [The ability to use location as a means to authorise mobile transactions would provide me with a better protection against fraud.]		
Answer	**Count**	**Percentage**
Strongly Agree (A1)	8	7.21%
Agree (A2)	38	34.23%
Neither Agree or Disagree (A3)	34	30.63%
Disagree (A4)	18	16.22%
Strongly Disagree (A5)	13	11.71%

Field summary for location7(SQ006)

Please state how much you agree or disagree with the following statements.
[The ability to use location as a means to authorise mobile transactions would provide me with a better protection against fraud.]

Answer	Count	Percentage
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for Summary1

Thankyou for completing this survey. If you feel there is anything wrong with the questions asked or indeed anything missing please can you feedback here.

	Count	Percentage
Answer Browse	18	16.22%
No answer	93	83.78%
Not displayed	0	0.00%

Field summary for Summary2

There will be an additional visual survey after this has been completed where visual imagery of a system that would allow you to control device location security. The aim is to provide a better understanding of how a system might work and guage you feedback. If you are happy to take part please can you leave your email address below and you will be contacted in due course.

	Count	Percentage
Answer Browse	36	32.43%
No answer	75	67.57%
Not displayed	0	0.00%

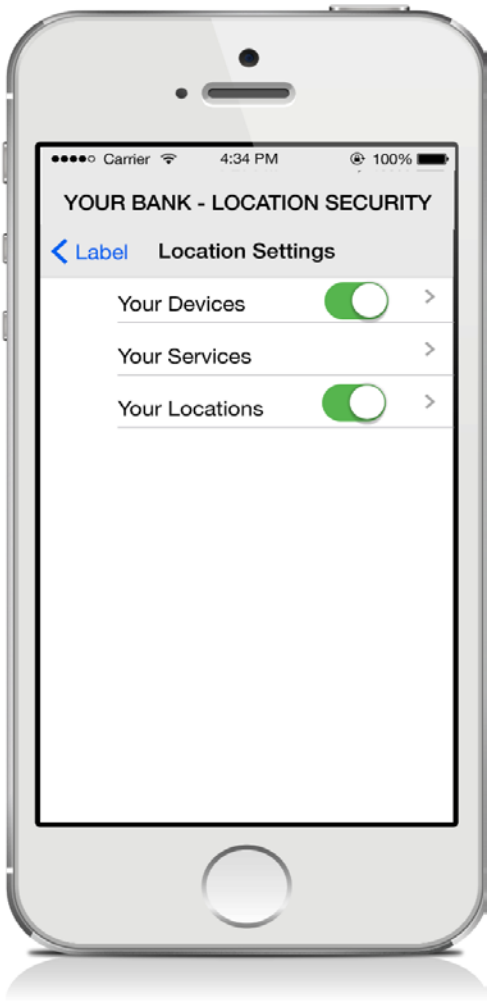
Appendix D – Secondary Survey Design

This survey will show you a selection of screens of an application (embedded within your banking application) that demonstrate how you can use location and device controls to authorise different forms of mobile transactions. It is not a completed application but merely an aid to help you understand more clearly how such an application may work and then ask your opinions on the functionality.

The purpose of the proposed application extension is to explore the feasibility of providing an additional level of security to protect against fraudulent attempts at using your financial information.

There is an assumption within the screens you see that you already signed into your banks mobile application.

Main Menu



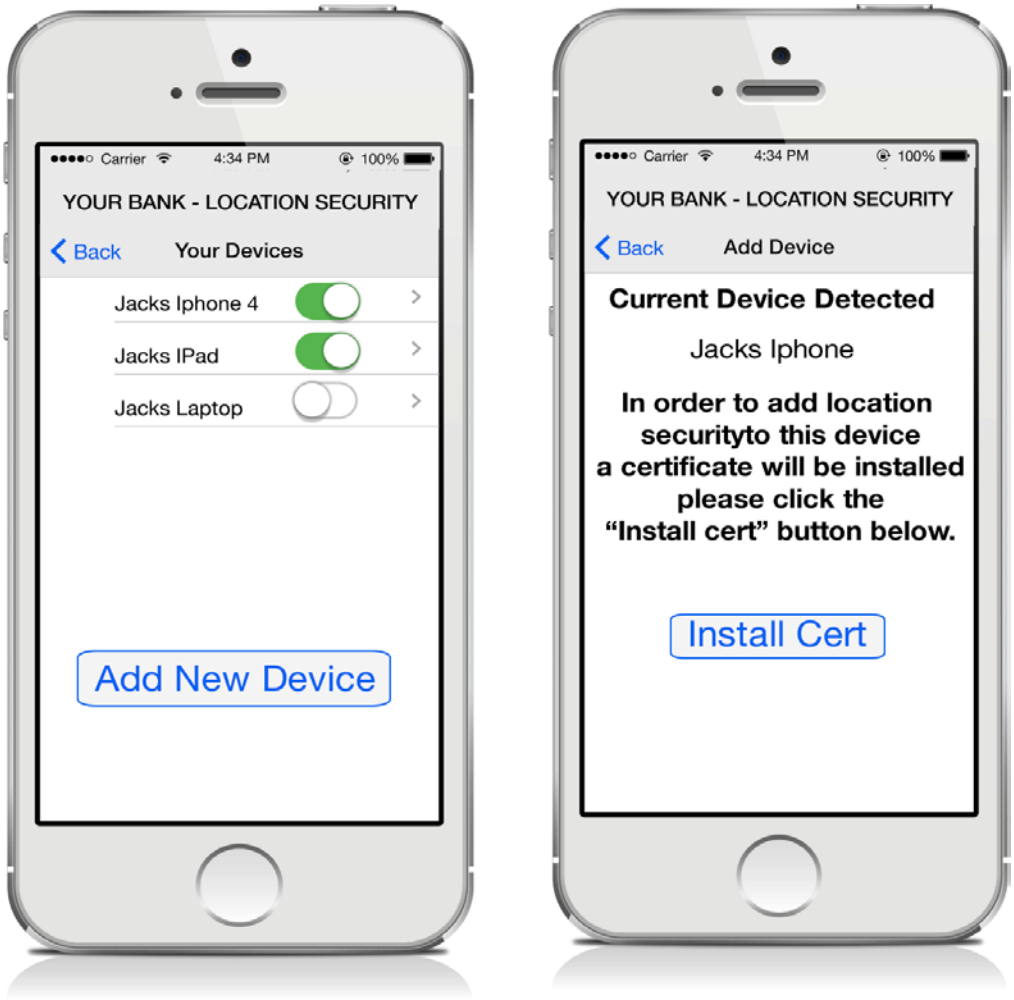
The menu on the screen provides 3 basic options:-

1) Access to your devices
2) Access to your services
3) Access to your locations

In addition the devices and location menus can be deactivated via the commonly used green toggle option. This provides you the flexibility of control over using not using either of these functions.

For example, you may wish to authorise transactions simply by where you are (i.e. locations). Alternatively you may only want to authorise your tablet for eBay purchases and may not be bothered about location of the device.

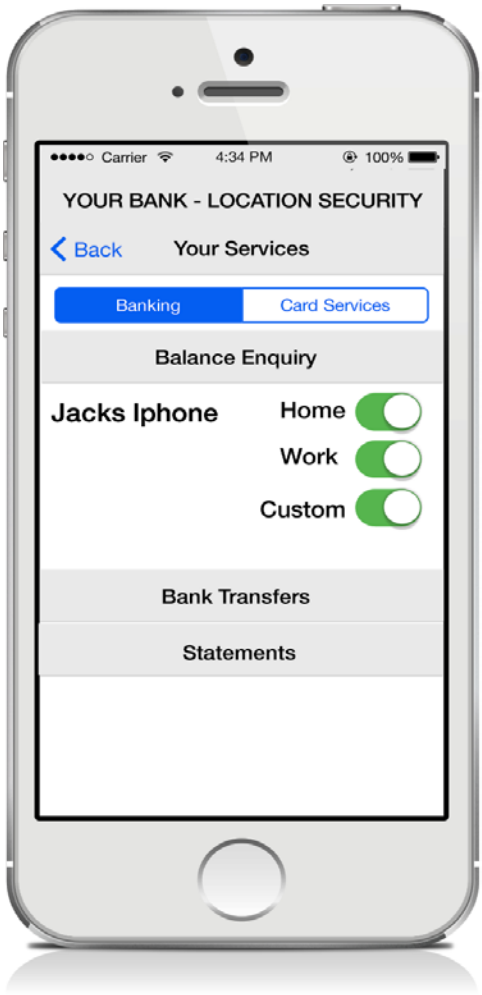
Device Menu Screen



The device menu allows you to register a new device as the example shows. This is done using the add new device button which in turn installs a certificate to the device that is used by the application to verify the source of the transaction.

Toggle options allow you to deactivate restrictions per device. The arrow would link you to the services screens. The navigation menu at the top of the application takes you back to the main menu for location services.

Service Menu Screen



The service menu allows you to set controls over what features you want to access. There are two main tabs, Banking, for the features you use in internet banking and card services for purchases made via your mobile devices.

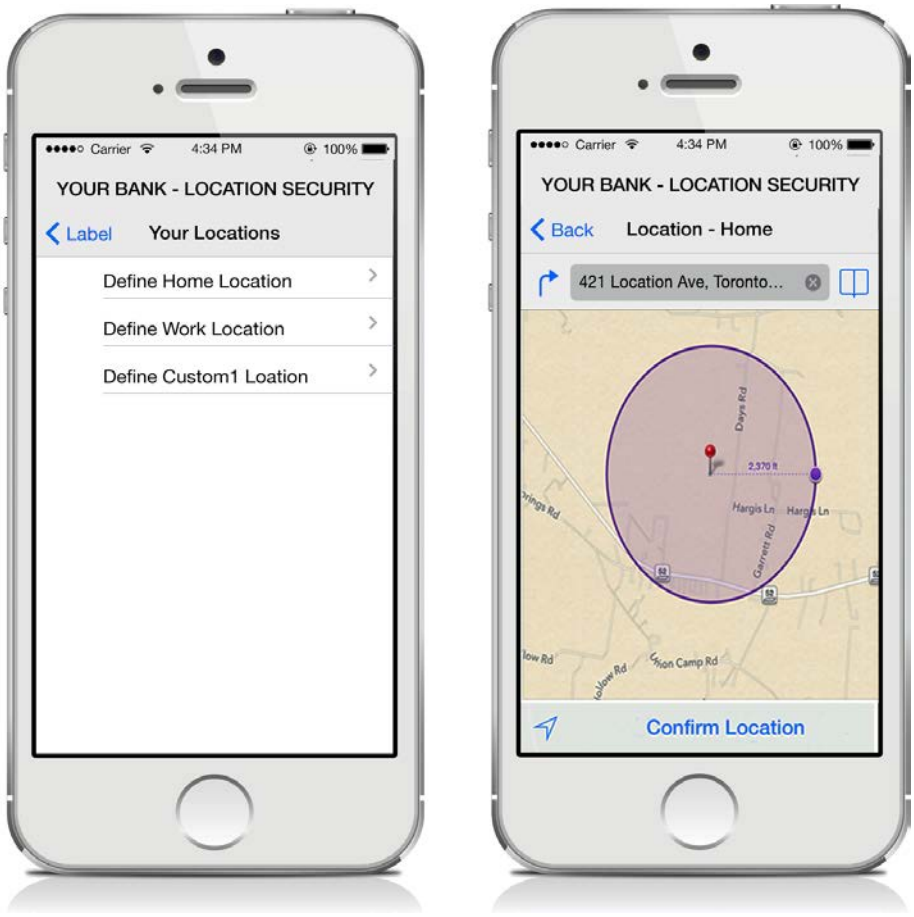
The example screen shows the banking layout. You would be able to select the banking function i.e. Balance Enquiry, Bank Transfer or Statements and the menu would show the devices available for that function.

So in this example Jacks IPhone can access Balance Enquiry from Home, Work and his Custom location. Simple use of the toggle switches allows any location to be disabled.

If devices were not being used in location settings then the locations would simply be available in each banking feature.

The same approach is considered for the Card Services tab. In this screen you would be able to restrict devices for mobile card purchases and/or mobile PayPal transactions.

Location Menu Screens



The location menu screens show how you could define each of the locations. There is also the possibility of enabling you to add multiple custom locations and naming them but for the purposes of the survey there are three simple areas, home, work and a custom defined location. Once you tap a location you are taken to the next map screen where you can find your location using typical mobile search parameters or using the find location arrow. You can then use gesture pinch controls on the phone to define an area for the location. Once happy with the area the confirm location would be selected.

The select areas are shown as gesture controlled circle radius. This approach has been taken, as GPS positioning may not always be accurate enough for a single pinpoint.

Appendix E – Application Survey

Results

Number of records in this query: 20

Total records in survey: 20

Percentage of total: 100.00%

Field summary for Priorview(SQ001)

Please state how much you agree or disagree with the following statements.

[Location may be useful in limiting fraud in ecommerce transactions.]

Answer	Count	Percentage
Strongly Agree (A1)	0	0.00%
Agree (A2)	17	85.00%
Neither Agree or Disagree (A3)	1	5.00%
Disagree (A4)	2	10.00%
Strongly Disagree (A5)	0	0.00%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for Priorview(SQ002)

Please state how much you agree or disagree with the following statements.

[Device usage may be useful in limiting fraud in ecommerce transactions.]

Answer	Count	Percentage
Strongly Agree (A1)	1	5.00%
Agree (A2)	15	75.00%
Neither Agree or Disagree (A3)	4	20.00%
Disagree (A4)	0	0.00%
Strongly Disagree (A5)	0	0.00%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for Main01(SQ003)

The following questions should be completed ONLY AFTER viewing the example screens for a proposed security application available at the following link http://www.hayhurst.co/screens . Further instructions will provided on the page. Please state how much you agree or disagree with the following statements.

[The ability of toggling device and/or location controls makes me likely to use as I can easily control the settings.]

Answer	Count	Percentage
Strongly Agree (A1)	7	35.00%
Agree (A2)	9	45.00%
Neither Agree or Disagree (A3)	4	20.00%
Disagree (A4)	0	0.00%
Strongly Disagree (A5)	0	0.00%
No answer	0	0.00%

Not displayed 0 0.00%

Field summary for Main01(SQ004)

[The process of adding devices appears too complex to use or would make me less likely to bother using the application.]

Answer Count Percentage

Strongly Agree (A1) 1 5.00%

Agree (A2) 2 10.00%

Neither Agree or Disagree (A3) 2 10.00%

Disagree (A4) 11 55.00%

Strongly Disagree (A5) 4 20.00%

No answer 0 0.00%

Not displayed 0 0.00%

Field summary for Main01(SQ005)

[The ability to toggle on/off individual devices registered makes the application more useful to me.]

Answer Count Percentage

Strongly Agree (A1) 7 35.00%

Agree (A2) 10 50.00%

Neither Agree or Disagree (A3) 3 15.00%

Disagree (A4) 0 0.00%

Strongly Disagree (A5) 0 0.00%

No answer 0 0.00%

Not displayed 0 0.00%

Field summary for Main01(SQ006)

[Restricting banking services per device in conjunction with location appears complicated and I wouldn't understand how to use this.]

Answer Count Percentage

Strongly Agree (A1) 2 10.00%

Agree (A2) 0 0.00%

Neither Agree or Disagree (A3) 1 5.00%

Disagree (A4) 13 65.00%

Strongly Disagree (A5) 4 20.00%

No answer 0 0.00%

Not displayed 0 0.00%

Field summary for Main01(SQ007)

[I would prefer to simply allow or disallow mobile banking over individual features.]

Answer Count Percentage

Strongly Agree (A1) 1 5.00%

Agree (A2) 3 15.00%

Neither Agree or Disagree (A3) 6 30.00%

Disagree (A4) 9 45.00%

Strongly Disagree (A5)	1	5.00%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for Main01(SQ008)

[Restricting services by location only would be enough for me rather than per device.]

Answer	Count	Percentage
Strongly Agree (A1)	1	5.00%
Agree (A2)	4	20.00%
Neither Agree or Disagree (A3)	6	30.00%
Disagree (A4)	9	45.00%
Strongly Disagree (A5)	0	0.00%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for Main01(SQ009)

[If my bank had to store my locations and devices to use this system I believe the fraud protection it offers me would be a greater benefit than the privacy concerns I may have about my location data.]

Answer	Count	Percentage
Strongly Agree (A1)	1	5.00%
Agree (A2)	11	55.00%

Neither Agree or Disagree (A3)	5	25.00%
Disagree (A4)	1	5.00%
Strongly Disagree (A5)	2	10.00%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for Main01(SQ010)

[Defining my locations with pinch gesture controls seems simple enough to use.]

Answer	Count	Percentage
Strongly Agree (A1)	6	30.00%
Agree (A2)	10	50.00%
Neither Agree or Disagree (A3)	3	15.00%
Disagree (A4)	1	5.00%
Strongly Disagree (A5)	0	0.00%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for Main01(SQ011)

[Would you use a similar system to this if your bank offered it?]

Answer	Count	Percentage
Strongly Agree (A1)	1	5.00%

Agree (A2)	17	85.00%
Neither Agree or Disagree (A3)	1	5.00%
Disagree (A4)	1	5.00%
Strongly Disagree (A5)	0	0.00%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for Main01(SQ012)

[If my bank offered better fraud protection benefits as a result of using this system I would consider using it.]

Answer	Count	Percentage
Strongly Agree (A1)	4	20.00%
Agree (A2)	15	75.00%
Neither Agree or Disagree (A3)	0	0.00%
Disagree (A4)	1	5.00%
Strongly Disagree (A5)	0	0.00%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for Main01(SQ013)

[If this application was separate to your banking application I would trust it less.]

Answer Count Percentage

Strongly Agree (A1)	5	25.00%
Agree (A2)	8	40.00%
Neither Agree or Disagree (A3)	5	25.00%
Disagree (A4)	2	10.00%
Strongly Disagree (A5)	0	0.00%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for Main01(SQ014)

[If the bank stored and analysed my usage data I would still use this application for the fraud protection benefits.]

Answer	Count	Percentage
Strongly Agree (A1)	1	5.00%
Agree (A2)	10	50.00%
Neither Agree or Disagree (A3)	5	25.00%
Disagree (A4)	4	20.00%
Strongly Disagree (A5)	0	0.00%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for Main01(SQ015)

[I am too concerned about privacy issues to consider using an application like this.]

Answer	Count	Percentage
Strongly Agree (A1)	1	5.00%
Agree (A2)	1	5.00%
Neither Agree or Disagree (A3)	5	25.00%
Disagree (A4)	9	45.00%
Strongly Disagree (A5)	4	20.00%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for Main01(SQ016)

[If this system was implemented in my banking application I would find it simple to understand and use.]

Answer	Count	Percentage
Strongly Agree (A1)	4	20.00%
Agree (A2)	11	55.00%
Neither Agree or Disagree (A3)	4	20.00%
Disagree (A4)	0	0.00%
Strongly Disagree (A5)	1	5.00%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for Main01(SQ017)

[This application would be too complex for me to bother using.]

Answer	Count	Percentage
Strongly Agree (A1)	1	5.00%
Agree (A2)	1	5.00%
Neither Agree or Disagree (A3)	0	0.00%
Disagree (A4)	12	60.00%
Strongly Disagree (A5)	6	30.00%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for Main01(SQ018)

[I can see the usefulness in using location this way to help reduce fraud in my transactions.]

Answer	Count	Percentage
Strongly Agree (A1)	1	5.00%
Agree (A2)	16	80.00%
Neither Agree or Disagree (A3)	2	10.00%
Disagree (A4)	1	5.00%
Strongly Disagree (A5)	0	0.00%
No answer	0	0.00%
Not displayed	0	0.00%

Field summary for Main01(SQ019)

[Using device controls seen in the proposed application to limit fraud attempts would be useful.]

Answer	Count	Percentage
Strongly Agree (A1)	1	5.00%
Agree (A2)	15	75.00%
Neither Agree or Disagree (A3)	3	15.00%
Disagree (A4)	1	5.00%
Strongly Disagree (A5)	0	0.00%
No answer	0	0.00%
Not displayed	0	0.00%