Smartphones allow people to portably perform diverse tasks such as checking e-mail, banking, and shopping so that smartphone users are more likely to transmit or store sensitive information on the device. Thus, a question arises: How do smartphone users protect the sensitive information being kept on the device? Usually, biometric authentication is presumed to be more secure regardless of convenience and usability. Biometrics are facial recognition, fingerprint, hand geometry, signature analysis, iris scanning, retinal scanning, and voice recognition. In the paper, a survey was conducted to examine mobile users’ perception on biometric authentication methods and their adoption.

KEYWORDS: Biometrics, Mobile, Users’ Perception, Adoption Decision

INTRODUCTION

How do you protect the sensitive information stored on your phone? When most people are asked the question, they simply reply, “I don’t.” Usually, people tend not to secure their phone with some form of authentication, mentioning it is a time-consuming process. They don’t see potential risks by leaving their device unsecured or they don’t want to remember another password. According to a study conducted by Microsoft Research, the average user has 6.5 passwords, each of which is shared across 3.9 different sites. Each user has about 25 accounts that require passwords, and types an average of 8 passwords per day (Florencio & Herley, 2007).

Curiosity is heating up for biometric security in smartphones. Biometrics is the science and technology of measuring and analyzing biological data. In the area of information technology, biometrics refers to technologies that measure and analyze human body characteristics, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements for authentication purposes. Particularly, mobile biometrics solution has been greatly developed as features and performance of smartphones have been rapidly upgraded. As mobility is becoming an increasingly important part of the biometrics, mobile biometrics should be investigated in greater depth to be utilized to the full potential (Benini, 2012).

According to Goode Intelligence, it is estimated that by 2018, 3.4 billion users will have biometric features on their mobile devices (Vrankuji, 2013). Currently, fingerprint unlock method is widely deployed for Apple iPhone as well as Android phone users while face unlock is...
feasible for smartphone users with the new Android Lollipop OS (Bhagavatula et. al, 2015; Perala, 2014). Recently, body paint based biometrics are developed for mobile users.

Clarke & Furnell (2005) studied on authentication of mobile users by conducting surveys to find out how many people actually secure their mobile phones. They examined the use of mobile devices, authentication methods, and users’ attitudes towards future security options. The majority of the respondents made significant use of the devices with clear demands for protection against unauthorized use. However, the use of the PIN-based authentication was problematic while a third of the respondents indicated that they did not use it at all.

The purpose of our study is to find out how people actually secure their smart phones such as PIN, password, swipe codes, and biometrics. Also, mobile users’ perception on different types of biometric authentication methods is investigated. Their attitude, intention to use, and adoption on the biometrics will be examined.

LITERATURE REVIEW

The advent of high speed communication networks and increased computing power has allowed for smartphones to be used for more than simply making calls. Traditionally services like e-commerce and e-banking were carried out on a user’s home computer but are now performed on smartphones.

With the increase in sensitive information transmitted and stored on a user’s smartphone, does the PIN authentication method provide a sufficient level of security? The PIN has dominated the authentication scene as the primary method of user authentication for mobile phones including smartphones. The use of the PIN based approach has its own set of vulnerabilities which stem from users themselves. These vulnerabilities come from users’ choosing PINs which are repetitive numbers (e.g., 1111 or 0000) or a set of numbers that can easily be linked to the users (e.g., birthday or address). Other weaknesses attributed to the PIN based approach are that users give their PINs to others and write their PIN numbers down to remember them (Furnell et. al., 2008). Because of such vulnerabilities in the PIN based authentication method, mobile users explored alternative authentication methods including biometrics.

According to Clarke & Furnell (2005), biometrics can be divided into two categories, behavioral and physiological. Behavioral biometrics relies on characteristics like the way an individual speaks or the way they keystroke or sign their name. Physiological biometrics involves the use of a physical characteristic of one’s body. Types of physiological biometrics include fingerprints, facial features, voice, hand geometry, iris, and retina. Biometrics is considered as a secure authentication since each user would have a unique characteristic. It also removes a critical factor of having the user remember a PIN.

Biometrics works to authenticate identity by measuring and verifying an individual’s unique physical characteristics such as fingerprints, hand and face geometry, or patterns found in the eye’s iris. Since these identifiers can’t be borrowed or stolen, biometrics provides identity authentication with a strong degree of confidence. According to Zalud (2012), iris Identification is reportedly the most unique among biometric choices and may be the most stable of all biometrics.
America is far from being at full capacity regarding biometrics in smartphones. It is found that other countries are already in full swing with biometrics like a fingerprint reader within their phone system. One reason for the delay in biometric cell phones reaching U.S. consumers is marketing strategy. In other countries, many cell phone manufacturers are anxious to expand product lines to attract more customers. In foreign markets, cell phone manufacturers sell directly to consumers. In the U.S., however, service providers sell the phones with the features the provider wants to offer. As a result, the biometrics market in the U.S. has been very slow to gain acceptance compared to foreign markets.

Recently, as fraud cases are rising for financial institutions, voice recognition technology can be reviewed to ascertain the identity of the caller to reduce the loss in the financial transactions. Moreover, mobile users are more concerned about the use of voice recognition technology with the use of installed apps (Masterson, 2014).

For the study, a survey is designed to gauge smartphone users’ awareness of the various biometric technologies. While some people might have encountered or heard of a form of biometrics like a fingerprint reader, most people might have never heard of hand geometry or signature analysis. Since the idea of using biometrics on a smartphone is relatively new, the survey also determines perceived usefulness on the level of security, and perceived ease of use, users’ attitude towards the various biometric methods, and users’ intention to use biometric methods.

HYPOTHESES/MODEL

The research model is derived from the Technology Acceptance Model (TAM) that was initially developed by Davis (1989). The authors adopted perceived usefulness and ease of use. Usefulness is translated as how secure the biometrics can supply (Bhagavatula et.al., 2015). Thus, the research model includes the perceived level of security. As shown in Figure 1, research model includes users’ perceived level of security for biometric methods, ease to use, users’ attitude, intention to use, and adoption.

Figure 1: Research Model
The hypothesis to test is that users’ perception for biometric methods in terms of the level of security and perceived ease to use determines user’s attitude, which decides users’ intention to use. Users’ intention to use biometric methods finally leads users to adopt them.

METHODS

The survey instrument is designed to have demographic data, users’ perception for biometric methods in terms of the level of security, perceived ease to use, attitude toward the biometric method, intention to use, and the actual adoption of the biometric methods. Demographic data was asked about age, gender, education, ownership of smartphone, smartphone usage, and operating systems installed on smartphone. Users’ perception for biometric methods in terms of the level of security, perceived ease to use, attitude toward the biometric method, and intention to use is measured for seven (7) different biometric methods, that is, facial recognition, fingerprint recognition, hand geometry, signature analysis, iris scanning, retinal scanning, and voice recognition. One (1) statement is asked to measure users’ perception on the level of security for seven (7) biometric methods. Respondents reply on a 5 point Likert scale, that is, one (1) for extremely not secure and five (5) for extremely secure. One (1) statement is asked to measure users’ perception on the ease of use for the biometric methods. Respondents reply on a 5 point Likert scale, that is, one (1) for extremely difficult and five (5) for extremely easy. One (1) statement is asked to measure users’ intention to use for the biometric methods. Respondents reply on a 5 point Likert scale, that is, one (1) for strongly agree and five (5) for strongly disagree.

RESULTS

A survey was conducted which garnered 158 respondents in which 12 respondents did not own a smartphone. The survey was administered online and through paper format onsite. Google Docs was used to create and distribute the survey online, which allowed to automatically record responses and directly analyze data in the Excel format ensuring data integrity. Out of 158 respondents, 42% of respondents were between the ages of 25-34, while 25% were between the ages of 18-24, and 18% were between the ages of 35-44. Additionally, 59% of the respondents were female while 41% of the respondents were male. 92% of respondents owned a smartphone while 91% subscribed to a data package attached to mobile services.
In terms of the usage, 97% of respondents used their phone for calling, 96% for texting, 91% for internet browsing, 87% for emailing, 66% for gaming, 61% for banking/financial transactions, 46% for e-commerce, and 17% for digital wallet.

**DISCUSSION AND CONCLUSIONS**

We are still working on Data Analysis, Discussion, and Conclusion.

**REFERENCES**


