

Consumers' Awareness of, Attitudes Towards and Adoption of Mobile Phone Security

Stewart Kowalski

Ericsson Research, Kista, Sweden

stewart.kowalski@ericsson.com

Mikael Goldstein

Migoli, Stockholm, Sweden

mikael.goldstein@telia.com

Abstract

Mobile phones are used frequently, and people keep them turned on for extended periods of time. In this paper we examine to what extent current mobile phone security functionality is adopted and also about interest in future authentication methods. A student survey was conducted (N = 97) targeting Swedish security students' awareness, attitudes and adoption of mobile phone security functionality. Also, ten retailers were interviewed about customers' mobile phone security attitudes when purchasing a mobile phone. Student respondents were classified according to a simplified version of Rogers' technology adoption model. The sample was biased: 16% were classified as "Early adopters" whereas 46% were classified as "Laggards". Half of the sample was below 30 years of age, four out of 10 were females; six out of ten had a subscription whereas four out of ten had pre-paid. Awareness of security functionality was poor. Respondents seemed unaware of any security functionality other than the PIN, and that there exists two levels of security, one protecting the SIM card (PIN code) and one protecting the handset (phone security code). PIN code authentication was adopted by 82% whereas a very modest adoption of the phone security code authentication was found (15%). 33% did not use it whereas approx. half of the sample was not aware of its existence. Users who refrain from using the PIN code considered it significantly more troublesome to enter it. Females were significantly more concerned about their mobile phone than males: 95% use the PIN code compared to 80% of the men. Users who had a subscription were significantly more interested in protecting their mobile phone against unauthorized usage than users who used pre-paid. Age significantly influences adoption of (new) technology, with younger people being more inclined to adopt innovations. Attitudes towards increased security were good in general, but attitudes towards biometrics were poor. The retailers claimed that customers did not ask about security issues. The need for further study to distinguish between adopting and accepting security functionality is discussed.

Key words: Security, mobile phone, PIN code, phone security code, technology adoption, service adoption, functionality adoption.

1. Introduction

Mobile phones are currently an integral part of everyday life for most people in Sweden. As mobile phones obtain more advanced functionality and contain more sensitive data, the need for security measures increases. During a typical year, more than 1 million mobile phones were stolen in Europe (TRAI 2004). With enhanced security measures, a stolen mobile phone may be made useless for the thief. The Personal Identity Number (PIN) protects the Subscriber Identity Module (SIM card) from unauthorized usage. The phone security code protects the phone/handset. PIN code authentication (if enabled) doesn't protect the mobile phone since it is possible to switch SIM card and then access the phone anyway. Phone code authentication (if enabled) is activated if the SIM card is replaced. The problem with both these authentication procedures is that they are only enabled when the phone is switched on. Most users however, have their handset switched on all the time and consequentially most phones are on when stolen. The PIN code (a 4-8 digit code, usually 4 digits long) may be entered erroneously three times before the lock function is invoked. We are interested in finding out how awareness, attitude and adoption/usage of security functionality are related.

Awareness (knowledge) about security functionality does not necessarily imply usage/adoption of it. In a survey performed by Clarke et al. (2002a, 2002b) 89% of the respondents knew about the PIN facility but only 56% used it. Two-thirds of those not using PIN (44%) considered it inconvenient. However, in Clarke's study, neither payment types (subscription/prepaid) nor adoption categories (Rogers 1995) were controlled for. Clarke et al. did study however, user attitudes to possible future security measures (authentication) through biometrics. Whereas PIN authentication is based on something the user knows, biometrics is based on something the user is (fingerprint, voice biometrics, ear geometry, facial recognition, iris scanning or typing style/keystroke dynamics). Clarke et al. concluded that a hybrid method of authentication, combining biometrics and PIN code, appears to be an acceptable future method for authentication. A study made by Furnell et al. (2000) concerning users' attitudes towards different authentication and supervision techniques shows that users seem to prefer the same authentication method when it comes to computers as with mobile phones. 90% of the respondents preferred passwords as a means of authentication although many would accept voice verification and fingerprint recognition as a way of authentication (68%-67%). Clarke et al. (2000a, 2000b) found that 74% were favourable towards fingerprint authentication whereas 55% were favourable towards voice print authentication. Iris scanning, facial recognition and keystroke dynamics were regarded as less attractive means of future authentication (44%-28%).

Furnell (2005) found that domestic Internet end-users in the United States did not actually understand security very well. For example, more than half of the respondents were not clear on the difference between anti-virus and fire-wall protection (an anti-virus program destroys a computer program usually hidden within another seemingly innocuous program that produces copies of itself and inserts them into other programs and that usually performs a malicious action; a fire-wall computer (software) prevents unauthorized access to private data (as on a company's local area network or intranet) by outside computer users). This had as a result that 67% either had no anti-virus software on their system at all or had not updated it within the previous week and that 72% lacked a properly configured firewall. This finding implies that awareness or attitudes as such may not suffice. Thorough understanding about how security functionality works may thus also be crucial before any adoption takes place.

How is adoption of mobile phone security functionality distributed across the population? Innovation diffusion theory aims at predicting the likelihood and the rate of an innovation being adopted by different adopter categories (Rogers 1995, Kaasinen 2005). Rogers defined five adopter categories: Innovators (2.5%) Early adopters (16%), Early majority (32%), Late majority (32%) and Laggards (16%).

Technology adoption (Rogers 1995) according to the diffusion model usually refers to the actual acquisition of a product, artefact or *method* in time among different consumer segments (purchasers). It's the process rate by which society (or a certain subgroup of society, like farmers or programmers) adopts an innovation, be it the mobile telephone or a new way of tending crops. In the current student survey, all respondents had already acquired the new technology artefact (the mobile phone). The Technology Acceptance Model (TAM) predicts whether users will adopt new technology (Davis 1989) and is based on Perceived Ease of Use and Perceived Usefulness (the degree to which a person believes that using a particular system is: free of effort/ enhance job performance). These will affect their intention to use the system and eventually actual usage. Adoption of mobile phone security functionality among different adopter categories is investigated in this paper.

2. The security student survey and the retailer interview

The aim of the survey was to explore the relationship between the mobile phone user's awareness, attitude and adoption of mobile phone security functions among different adopter categories. Do end-users understand security functionality? To what extent is security functionality used? What interest is there in existing and future security functionality? The purpose is to understand, describe and predict mobile phone security behaviour.

Some of the hypotheses were:

- Does knowledge of the functionality affect the attitude towards security functionality?
- Does knowledge of the functionality or knowledge of security risks increase adoption of security functionality?
- Does awareness of security functionality increase adoption?
- Is security adoption level the same for different customer segments (do Early adopters adopt security functionality more quickly than other segments?)

A paper-based questionnaire based on the Clarke et al. (2002a) study was handed out to students who:

- 1) Attended a class in a security course at the IT University (Department of Computer Systems and Science), Sweden, held by one of the authors in the spring of 2003 (opportunistic sampling)
- 2) Owned a GSM phone (Global System for Mobile Communications, not a 3G (3rd Generation) or a GPRS-enabled phone).
- 3) Each respondent was screened by a questionnaire pinpointing his customer segment affiliation according to Rogers' (1995) consumer adoption model using a black-box approach.

Ten retailers in Stockholm, Sweden, were interviewed about customer attitudes towards mobile phone security when purchasing a phone.

3. Results

3.1 Descriptive statistics

97 security students participated in the survey. Age was distributed app. equal amongst those that were below/above 30 years of age. Most respondents were about 25-30 years of age. 40 percent were female. App. 6 out of 10 had a subscription whereas 4 out of 10 had pre-paid. Roger's five consumer segments were collapsed into three: Early adopters (including Innovators) (16%), Majority (Early and Late) (37%) and Laggards (46%). The sample distribution for security students did not match Rogers' consumer segment distribution; Laggards were over-represented and the Majority was under-represented.

3.2 Awareness of security functionality in the mobile phone

When asked about the two authentication concepts employed in mobile phones, the answers showed that the security students were not knowledgeable about them. 43% knew about the authentication for the SIM card concept (i.e. the PIN code) and 32% knew about the authentication for the mobile phone concept (i.e. the security code). Actually, 45% of the respondents claimed that their mobile phone did not have the security code function at all, which means that almost half of the respondents/users were unaware of the function.

However, 82% used the PIN code, so what they probably didn't know was the exact purpose of the PIN code. 32% were aware of the phone security code (but did not use it). Only 15% used it.

3.3 Attitudes towards current and future mobile phone security

Regarding trust in PIN code, only 54% of the respondent claimed to trust the protection offered by the PIN code. Very few, only 15%, regarded it inconvenient to enter the PIN code, which differs from the Clarke et al. (2002a) study, where 41% regarded it inconvenient.

Most (app. 70%) were positive towards increased security for mobile phones, with only about 25% regarding it as "unnecessary". Regarding positive attitude for biometric authentication methods, the different methods were ranked according to the following: fingerprint scanning (58%), voice recognition (38%), typing pattern (18%), ear geometry (16%), face recognition or iris scanning (12%). Missing values were in the order of 10-20%). The rank order roughly matches that obtained by Clarke et al. (2002a) (except for iris scanning (ranked 3rd) but the magnitudes of the positive answers were higher). When asked if the different biometric authentication methods could replace the PIN code, most respondents were not particularly interested in the alternative methods. Only fingerprint scanning and voice recognition were regarded as satisfactory substitutions (54 and 40%).

3.4 Current adoption of mobile phone security functionality

82% used their PIN code whereas approx. half of the respondents were not aware of the mobile phone security code. Of the remaining part, only one third (15%) used it whereas two thirds (32%) were aware of it but did not use it. About one third of the respondents had disclosed their PIN to somebody else. About 78% used their mobile phone on a regular basis for private calls and approx. half of them sent SMS daily.

3.5 Inferential statistics regarding gender, subscription type, age and consumer segment

Several null hypotheses were tested for significance by means of chi-square testing. The chi-square test compares the observed data with a null hypothesis to see if the data deviates from a roughly even distribution between the cases. The null hypothesis is called "null" because it

states that there will be no deviation (e.g. “there is no relation between age and adoption level”). If the null hypothesis holds, the data should be evenly distributed. The chi-square test calculates if the data is evenly distributed and how much it deviates. If the data is unevenly distributed, the null hypothesis is false and you have significance (significance level 5%).

Gender affects PIN code usage. Female users were significantly ($\chi^2 = 4,375$, $p = 0,036$) more concerned about their mobile telephones than male users, as almost all the females use the PIN code compared to about 4/5 of the men. This was the only significance shown when gender was cross-tabulated with any other variable.

Type of subscription affects interest in security. Users who have a subscription were significantly ($\chi^2 = 9,94$, $p = 0,02$) more interested in protecting their mobile phone against unauthorized usage than users who used pre-paid. This is probably a natural consequence of their larger investment and greater economic risk.

Users who don't use the PIN code regarded it as significantly ($\chi^2 = 5,572$, $p = 0,018$) more troublesome to enter, and that is probably the reason why they did not use it.

The SMS function was used significantly ($\chi^2 = 10,039$, $p = 0,007$) more in the younger age group (<30 years) where two thirds sends/receives more than one SMS per day.

The older age group (>30 years) was significantly ($\chi^2 = 7,344$, $p = 0,007$) more interested in ear geometry than the younger age group (<30 years).

Age appears significantly ($\chi^2 = 8,149$, $p = 0,017$) to influence adoption of technology. Young people (<30 years) are overrepresented in the Early adopter segment and underrepresented in the Laggards segment. However, according to Rogers (1995), no research clearly supports the theory that young people are earlier technology adopters than older.

The consumer segment classified as Early adopters were significantly more favourable to the biometric authentication method voice recognition ($\chi^2 = 7,757$, $p = 0,021$).

3.6 The retailer interviews

The following summarizes the interviews with the 10 retailers:

Customers do not ask about mobile phone security issues. Customers are not interested in security. They are less interested if they buy a low-end phone or if they purchase a company phone, since the economic risk is with the company. What customers are concerned with are stand-by battery time, functionality and pricing. All retailers sold mobile phone insurance, but one. The customer usually only bought a special insurance when purchasing a high-end phone with subscription.

4. Discussion

Security functionality does not seem to follow the path of technology adoption when it comes to diffusion among consumer segments. Awareness as well as proper understanding of security functionality concepts must be taken into consideration before any true adoption of security functionality is likely to occur. It appears that technology device adoption per se does not automatically imply security functionality adoption. The adoption of security functionality in this study is in accordance to what others have found (Clarke et al. 2002a, 2002b, Furnell 2005). The most important challenge is to let the security functionality take into account the

fact that the mobile phone is always on, which favours biometric authentication methods. However, the current security functionality methods PIN code and phone lock which both are enabled when the phone is switched on and if the SIM card is replaced, has to be properly understood by the end-user. The security measures were not designed to deal with the fact that mobile phones are always on and that biometrics techniques may be favourable to deal with this issue. But before biometrics can be introduced, both awareness and attitudes has to be dealt with in order for the functionality to be adopted and used correctly.

When it comes to technology usage, there appears to be a distinction in the literature between acceptance and adoption models. Whereas Rogers (1995) speaks about technology *adoption* Davis (1989) speaks about technology *acceptance* in the Technology Acceptance Model (TAM). The TAM has been applied mostly in studying office software usage whereas innovation diffusion theory aims at predicting the likelihood and the rate of an innovation being adopted by different adopter categories on a free consumer market. The contexts in which the two theories are used differ substantially: In a large company introducing a new email system (Hubona and Burton-Jones 2003) the user does not actually have a choice regarding using/not using the system, so the term acceptance is more appropriate. The employee might be using the software without believing in its benefits (e.g., the product's/system's Perceived Usefulness (Davis 1989)). As a consumer on a free market, the customer has a free choice of adopting/not adopting new technology and here the term adoption is more appropriate to use, since he adopts using it out of believing that it will useful to him.

People might actually use technology without believing in it. This should be referred to as technology acceptance. Individuals that both believe in and use the technology we refer to as adoption. This distinction is reflected in the current survey by the fact that 82% used the PIN code but only 54% trusted the PIN code. Thus users that trust *and* use something are adopting it, whereas those that use the function and don't trust it are only accepting it. The distinction between adoption and acceptance might give future indications regarding who is willing to pay for security functionality. Further research has to be done in order to analyze the distinction between acceptance and adoption.

Another area of future research targets the distinction between product adoption, service adoption and (security) functionality and feature adoption. When purchasing a mobile phone, the artefact may be regarded as an enabler. Zeithaml (1981) makes a distinction between adoption of products and services, stating that service innovations are adopted more slowly. Whereas services are intangible, inseparable, heterogeneous and perishable the opposite applies to goods (e.g., a mobile phone). The service cannot be seen, tasted, felt or heard before it is bought. The intangible nature of services makes it difficult for customers to evaluate the service prior to purchase and therefore service purchase may be considered risky. To reduce risk customers may focus on tangible cues such as brand. A further distinction may be thus added, the adoption of security functionality. The intangible nature of some of the mobile phone security functionality is evident. By introducing fingerprint recognition in mobile phones, security functionality may become indeed become more tangible, which will increase usage.

5. Acknowledgements

We wish to thank Carina Bergman and Björn Carlberg, students at the IT University in Stockholm, for constructing the questionnaires and collecting and analysing the data.

References

- Clarke, N.L, Furnell, S.M, Rodwell, P.M and Reynolds, P.L (2002a). Acceptance of subscriber authentication methods for mobile phone devices. *Computers & Security*, 21, 3, 220-228.
- Clarke, N.L, Furnell, S.M and Reynolds P.L (2002b). Biometric authentication for mobile devices. *3rd Australian Information Warfare and Security Conference*, 2002.
- Davis, F.D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology, *MIS Quarterly*, 13, 319-339.
- Furnell, S.M, Downland, P., Illingworth, M.M. and Reynolds, P.L. (2000). Authentication and Supervision: A Survey of User Attitudes. *Computers & Security*, 19, 6, 529-539.
- Furnell, S.M. (2005). Why user cannot use security. *Computers & Security*, 24, 274-279.
- Hubona, G.S. and Burton-Jones, A. (2003). Modeling the User Acceptance of E-Mail. *Proceedings of the 36th Hawaii International Conference on System Sciences*, HICSS'03,
- Kaasinen, E. (2005). *User acceptance of mobile services-value, ease of use, trust and ease of adoption*, Espoo 2005, VTT Publication, 566, Finland.
- Rogers, EM (1995). *Diffusion of Innovations*, Fourth edition, New York, Free press.
- TRAI (2004). Telecom Regulatory Authority of India website. Available at: <http://www.trai.gov.in/annexure.pdf> (January 2004).
- Zeithaml, V.A. (1981). How consumer evaluation processes differ between goods and services, In: *Marketing of Services*, by James H. Donnelly and W.R. George (Eds.), Chicago, IL: American Marketing Association, 186-190.