Smartphone Deployment of Keystroke Analysis

A.Buchoux and N.L.Clarke

Centre for Information Security and Network Research,
University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

The current security on mobile phones is often limited to the Personal Identification Number (PIN) which is a secret-knowledge technique. Studies highlighted the drawbacks of such a method. The technologies on such devices are likely to evolve fast. As an example, a lot of handsets enable online banking or shopping nowadays, which can involve the storage or processing of sensitive data. The security on such devices should be effective to prevent impostors to use them. This study proposes an enhanced technique for authentication on Smartphone using keystroke analysis. Results of a practical evaluation are presented based upon the entry of a password which can be either number or character-based. The findings reveal the technique employed is not yet ready to be deployed on the market as the performance rates are relatively poor. However, it suggests that this biometric technique could be utilised on a mobile device as the processing requirements of the algorithms used are low. Furthermore, this study collected the participants' thoughts and reactions about the system which were interesting to discuss.

Keywords

Keystroke analysis, authentication, biometrics, Smartphone, mobile devices

1 Introduction

Mobile devices and more specifically Smartphone are allowing access to a large variety of services. Users can now pay products directly on their devices, visit web pages or consult their bank account. Along with this services enhancement, handsets have built-in technologies that allow faster access to the network, larger storage space and multimedia functions. Such services generate sensitive information with for instance bank account details, passwords or other private information. Moreover, the storage space growth enables users to store more and more data on their handsets; this information could be in danger if no good security measures were applied. The current sales of Smartphone are rising according to Gartner (Pettey, 2008) with a sales growth of 29.3 percent in the first quarter of 2008 compared to the same period last year. If no adequate authentication security is enabled on them, it could reveal a high number of potential unsecured devices on the market. Therefore, a lot of personal data – and maybe professional data, as this type of handset is popular among companies' employees – could be in danger.

The current and most common mobile phone security system is the Personal Identification Number (PIN). Such a system is based upon a secret-knowledge approach and relies on the user to ensure the device's security. Effectively, the PIN needs to be kept secret in order to be efficient; if an impostor discovers it, she/he can be authenticated successfully and for instance read potentially sensitive information. A mobile handset with the PIN security enabled can be considered more secured than a handset with no security at all. However, a survey conducted by Pointsec Mobile Technologies (2005) revealed that a third of surveyed people did not use a PIN. Moreover, Clarke and Furnell (2005) also found out that approximately a third of people did not use the PIN security. It means that a lot of users' devices are not protected. If it was stolen or lost, the handset services would be usable by anyone and the data could be misused.

As knowledge-based methods might not be appropriate to protect mobile devices, other types of authentication should be worth looking at. Among the different techniques, three means are to be detailed (Wood, 1977). The first one is to use something the user knows to authenticate. The PIN is embedded into this category, as well as the password. The second category uses something the user has such as a token. Finally, the third category utilises something the user is. The latest is the one that interests the authors. This category is commonly known as biometrics and it exploits the user's characteristics. Moreover, two types of biometrics can be distinguished based upon the features it uses: physiological biometrics that identify a user based on the parts of her/his body; behavioural biometrics that use the way a user is (Jain et al., 2004). Keystroke analysis is a type of behavioural biometrics as it authenticates a user based upon her/his typing pattern. A major difference between those two techniques is that a physiological trait is likely to remain quite stable, whilst a behavioural characteristic is likely to vary if the environment or the user changes. Furthermore, all current keystroke analysis studies on mobile platforms relied upon a network-based method; this project seeks to deploy a standalone authentication technique on a Smartphone. Therefore, the pattern classification algorithms will be executed on the device and not on a remote server.

This paper begins with section 2, describing background literature which helps to provide general information about biometrics, the pattern classification process and keystroke analysis. Then, the methodology is detailing the steps of the study from the software implementation to its evaluation. The results are presented in the fourth section. These include the processing requirements, the classifiers performance and the questionnaire results. The following section discusses these results and to finish a conclusion sums up the main findings and the potential future research.

2 Background literature

Biometrics can be used as a mean to identify people. Each technique has its own characteristics, and its own performance rate. Several rates can be utilised to choose a biometric technique. There are three common terms that are the False Acceptance Rate (FAR), the False Rejection Rate (FRR) and the Equal Error Rate (EER). The FAR measures the rate at which an impostor is able to authenticate. The FRR describes the rate to which a genuine user is not able to be authenticated. The EER is the rate when the previous two values cross and is often used as a way to compare biometric techniques.

Keystroke analysis is one of the numerous biometrics. It aims at identifying a user based upon her/his typing pattern. It is a fairly promising technique on Smartphone, because the cost of the implementation is reduced by the fact that the only hardware required – the keypad or keyboard – is already available on the device. Among the different inputs the user provides, the system usually collects two different features: key press and key release times. These values are then assembled into digraphs, trigraphs or more. The difference between those is the number of keys considered; a digraph is the features of two keys while a trigraph is the features for three keys. Based upon these values, the system will then calculate some other features. They are commonly known as the hold-time which is the difference between a key release and a key press, and the inter-keystroke latency which is the time between two consecutive keystrokes. The latter is considered as the most discriminative of the user's behaviour. Moreover, there are two types of keystroke analysis. The first one is static analysis and is based upon static text. It is relatively suited to authentication and the password will be considered as the static text. The second type is dynamic analysis and is related to the entry of free text (Bergadano, 2003). With the latter, the user's samples can be captured in the background which enhances the convenience. However, it makes the process more difficult to achieve in practice especially because more user samples are required (Dowland and Furnell, 2004). The enrolment takes more time therefore the device security is not ensured during this long process.

Study	*FAR (%)*	*FRR (%)*	*EER (%)*
Anagun (2002)	4.6	1.2	N.A.
Bergadano et al. (2003)	5.36	0	N.A.
Cho et al. (2000)	0	19.5	N.A.
Clarke and Furnell (2007a)	N.A.	N.A.	13
Clarke and Furnell (2007b)	N.A.	N.A.	4.9
Clarke et al. (2003)	11.7	10.9	11.3
Guven and Sogukpinar (2003)	1	10.7	N.A.
Monrose and Rubin (1997)	N.A.	9.3	N.A.

Table 1 - Neural network studies performance rates

There are a lot of studies that evaluated keystroke analysis. However, only a few of them considered its application to mobile devices (Clarke et al., 2003; Clarke and Furnell, 2007a; Clarke and Furnell, 2007b). Therefore, other studies assessing keystroke analysis on PC-based environments are to be considered. It seems that a lot of studies assessing both static and dynamic keystroke analysis found out that dynamic analysis was less likely to achieve good error rates compared to static analysis (Monrose and Rubin, 1997; Clarke and Furnell, 2007a; Clarke and Furnell, 2007b). Moreover, a lot of differences can be shown considering the pattern recognition algorithms. Effectively, their choice is very important as it will decide the performance rates of the solution. The majors classifiers are either statistical, Bayesian or neural networks. Generally, the results for statistical algorithms are not suitable for use on a real device: Monrose and Rubin (1997) achieved 9.3 percent FRR, Bergadano et al. (2003) achieved 5.36 percent FAR at zero FRR and Guven and Sogukpinar (2003) revealed 1 percent FAR at 10.7 percent FRR. However, neural networks seem to be interesting as it can be seen in Table . The feed forward multi-layered perceptron (FF MLP) with backpropagation neural network is especially chosen by studies (Cho et al., 2000; Anagun, 2002; Clarke et al., 2003; Clarke and Furnell, 2007a; Clarke and Furnell, 2007b). The results might suggest that this classifier is usable in real conditions on mobile devices. However, neural networks are known to require a lot of processing power which might be a problem on mobile devices.

3 Methodology

This study seeks to implement keystroke analysis on a Smartphone. Therefore, a software program has to be implemented. The programming language is Visual Basic .NET and uses the Microsoft .NET Compact Framework 2.0. This framework is quite handy as it supports several programming languages and mobile operating systems. Therefore, a unique program will be able to run on Microsoft Windows Mobile 5 or 6. The software program is divided into two different forms: one for enrolment and one for authentication. Two types of password were proposed which were a simple PIN or a strong alphanumeric password. The password textboxes in these forms capture key events and the inter-keystroke latencies are saved on the handset. Moreover, three classifiers are evaluated based upon prior results; the Euclidean distance, the Mahalanobis distance and the FF MLP neural network. The first two algorithms are statistical-based methods which are likely to have low processing requirements, which is important on a mobile platform such as a Smartphone. The neural network technique is more likely to have high processing requirements, but its performance rates are usually better.

Figure 1 - Evaluation handset: SPV C600

A group of twenty people evaluated the software. In one session, they were asked to enrol by entering twenty times their password and authenticate ten times (see forms on Figure 2). A SPV C600 Smartphone running Microsoft Windows Mobile 5 was used (see Figure). It has a 195 MHz TI OMAP850 processor and 64 Mb of RAM. The enrolment and authentication samples were saved for further calculation of performance rates. Then, they filled a questionnaire assessing their general use of mobile devices, their biometrics knowledge and the software usability. Some of the key questions were concerning the enrolment process, the authentication process, the ease of use or some critics they wanted to formulate.

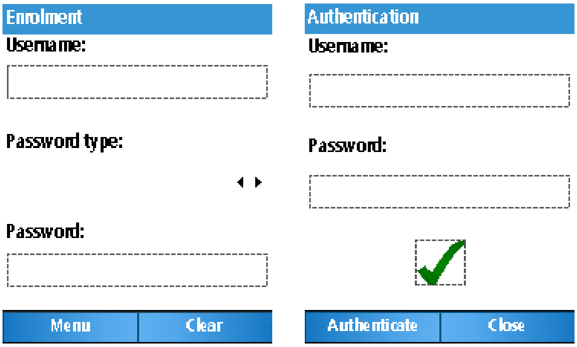

Figure 2 - Software program forms

4 Results

The study and the evaluation revealed the feasibility of keystroke analysis on a Smartphone environment. Effectively, such devices are limited in processing capacity. Therefore, the processing requirements of classifiers should be as low as possible. The two statistical techniques were not a problem as the enrolment was done in less than two seconds, with no reliance upon the number of samples or password-length. The enrolment process length for such classifiers should be reduced to the time taken to enter the password samples. However the neural network showed, as expected, high processing requirements. Its characteristics were minimal due to the processing time: ten neurons in the hidden layer and a hundred training iterations. The enrolment took three minutes and a half for twenty samples and a ten keystrokes length password. The authentication took approximately five seconds.

The different classifiers performances were assessed for random threshold values. Figure 3 shows the performance rates for the Mahalanobis algorithm. The Euclidean classifier performance rates are described in Figure 4.

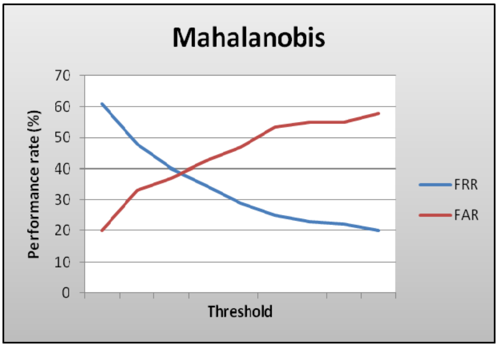

Figure 3 - Mahalanobis performance graph

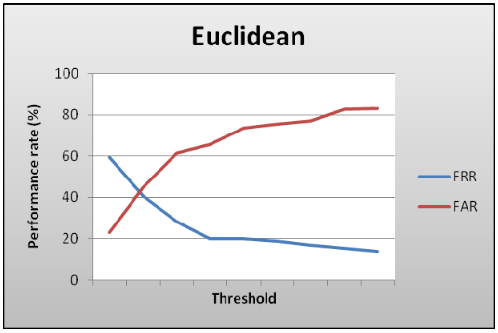

Figure 4 - Euclidean performance graph

The second section of the evaluation, the questionnaire, exposed the participants' thoughts about their knowledge and software usability. First of all, they answered to general questions about their mobile device use. Seven out of 20 participants do not use any security measure on their handset and fifteen users think that their device information is sensitive. Two participants used both PIN and password techniques which explains the total number of answers which is greater than 20. Moreover, five out of the seven participants who did not use any security feature think their information is sensitive. Then, they assessed the study software program usability. 19 users think that the software is easy to use and half of them found the enrolment time consuming. One user thought that the enrolment was both time consuming and easy to go through. The participants justified the length of the process by the number of samples that needed to be entered. Effectively, they estimated that 20 samples were too much to enter and were quickly bothered by the repetitive task. The other half of the users found out that the enrolment was easy to go through. Overall, 18 participants would use the solution if available and all of them thought it would provide more security.

5 Discussion

The system seems to be time consuming, especially for enrolment as pointed out by half of the participants. The fact that enrolment only occurs one time should be taken into account. This might suggest that the method is not as time consuming when it is used a long time. However, measures could be taken to shorten its duration. Effectively, the enrolment samples number could be reduced on a user basis: the shorter the password is, the fewer samples are needed because the latency times will be more regular than with a long password. It might help to decrease the time required for enrolment. Moreover, the FF MLP neural network classifier was not convincing. It should be noted that the algorithm was perfectible and that errors might reside in it. On the other hand, the processing requirements highlights that such a technique is hardly implementable on a Smartphone. For instance, three minutes and a half for enrolment is quite long, but not extremely. It should be worth noticing that the real neural network characteristics were not applied: the network should be between 100 and 500 neurons in the hidden layer and between 1 000 and 10 000 iterations. Even if only the number of iterations was changed to a thousand, it should extend the enrolment time by ten times; therefore the enrolment would approximately take thirty-five minutes. It seems impossible to lock out the user for such a time. Even if run in background mode, the process/thread priority should be reduced in order to keep the Smartphone running smoothly, which would increase this theoretical enrolment time. That is why neural network seems hardly achievable on a mobile device, while the statistical classifiers run very well on such a handset. However, their performance rates are not good enough to be run on a real device. The processing requirements might be not as restrictive on more recent devices as on the SPV C600 device which is quite old today. Some strong programming techniques should be used when implementing a neural network classifier on a mobile platform to reduce its processing requirements as much as possible.

The participants' comments gave a clearer view on their mobile use. Therefore, the fact that seven of them do not use any security measure is quite alarming. That is to say approximately two thirds of them do not protect their data. However, five of those seven participants think their information is sensitive. It might suggest that the current security measures are not suited to their need, or that they do not want to bother with security even if they know it is dangerous for their data. The reasons they did not protect their device was either because it was time consuming or too difficult to use. Therefore, the fact that half of them thought enrolment was time consuming should restrain them from using this security technique. That was not the case as 18 of them would use it and all of them thought it provided more security. Overall, it seems encouraging that they are willing to use new security solutions. Moreover, the fact that they think their information is sensitive – even for those not using security solutions – is interesting: they know that they should pay more attention to their data. Therefore, it could be said that their security awareness is good but that the current security techniques put in place are not suited to their needs or abilities.

6 Conclusion and future work

This study showed that keystroke analysis should be implementable on a mobile handset. The statistical classifiers demonstrated low processing requirements and can be used on a real device. On the other hand, the performance rates were not usable in practice. A far more promising technique, neural networks, was requiring too much processing power for such a platform. However the technique is promising and the participants' comments were rather encouraging. Therefore, they are seeking for other security settings on their mobile phones and would like new authentication techniques. Even if they suggested that this method was time consuming at enrolment, they wish they could use it on their handset. Overall, it could suggest that new approaches should be worth investigating in the authentication field.

This study highlighted several restrictions. For instance, the biometrics samples were not encrypted, which might increase the risk for identity theft. Privacy should be ensured by using cryptography when storing those samples. Then, it could be worth trying to integrate the solution to the Microsoft Windows Mobile security architecture. Effectively, the software program of this study was a standalone application. The security architecture of Windows Mobile provides what is called the Local Authentication SubSystem (LASS) which helps programmers to integrate their authentication systems to the environment. Moreover, this study focused on Microsoft mobile environments and it should be interesting to investigate other systems such as BlackBerry or Symbian. Finally, a neural network might be implemented with care to the processing requirements.

7 References

Anagun, A.S. (2002) 'Designing A Neural Network Based Computer Access Security System: Keystroke Dynamics and/or Voice Patterns' *International Journal of Smart Engineering System Design*, 4 (2): 125-132.

Bergadano, F., Gunetti, D., and Picardi, C. (2003) 'Identity verification through dynamic keystroke analysis', *Intelligent Data Analysis*, 7(5): 469-496.

Check Point Software Technologies LTD. (2005) 'IT Professionals Turn Blind Eye to Mobile Security as Survey Reveals Sloppy Handheld Habits', *Check Point Software Technologies*, [online] Available HTTP: http://www.checkpoint.com/press/pointsec/2005/11-18.html [accessed 20 July 2008].

Cho, S., Han, C., Han, D.H. and Kim, H.I. (2000) 'Web-Based Keystroke Dynamics Identity Verification Using Neural Network' *Journal of Organizational Computing and Electronic Commerce*, 10 (4): 295-307.

Clarke, N.L, Furnell, S.M., Lines, B.M., and Reynolds, P.L. (2003) 'Keystroke dynamics on a mobile handset: a feasibility study', *Information Management & Computer Security*, 11 (4): 161-166.

Clarke, N.L., and Furnell, S.M. (2005) 'Authentication of users on mobile telephones – A survey of attitudes and practices', *Computers & Security*, 24 (7): 519-527.

Clarke, N. L. and Furnell, S.M. (2007a) 'Advanced user authentication for mobile devices' *Computers & Security*, 26 (2): 109-119.

Clarke, N. L. and Furnell, S.M. (2007b) 'Authenticating mobile phone users using keystroke analysis' *International Journal of Information Security*, 6 (1): 1-14.

Dowland, P. S. and Furnell, S.M. (2004) 'A Long-Term Trial of Keystroke Profiling Using Digraph, Trigraph and Keyword Latencies', in: *Security and Protection in Information Processing Systems*, Springer, Boston: 275-289.

Guven, A. and Sogukpinar, I. (2003) 'Understanding users' keystroke patterns for computer access security' *Computers & Security*, 22 (8): 695-706.

Jain, A.K., Ross, A., and Prabhakar, S. (2004) 'An Introduction to Biometric Recognition', *IEEE Transactions on Circuits and Systems for Video Technology*, 14 (1): 4-20.

Monrose, F. and Rubin, A. (1997) 'Authentication via Keystroke Dynamics' *Proceedings of the ACM Conference on Computer and Communications Security*, ACM, New York: 48-56.

Pettey, C. (2008) 'Gartner Says Worldwide Smartphone Sales Grew 29 Percent in First Quarter of 2008', *Gartner*, [online] Available HTTP:

http://www.gartner.com/it/page.jsp?id=688116 [accessed 20 July 2008].

Wood, H.M. (1977) 'The use of passwords for controlled access to computer resources', *National Bureau of Standards,* Special Publication 500-9.