

Deployment of Keystroke Analysis on a Smartphone

A. Buchoux¹ and N.L. Clarke^{1,2}

¹Centre for Information Security & Network Research,
University of Plymouth, Plymouth, UK
info@cisnr.org

²School of Computer and Information Science, Edith Cowan University,
Perth, Western Australia

Abstract

The current security on mobile devices is often limited to the Personal Identification Number (PIN), a secret-knowledge based technique that has historically demonstrated to provide ineffective protection from misuse. Unfortunately, with the increasing capabilities of mobile devices, such as online banking and shopping, the need for more effective protection is imperative. This study proposes the use of two-factor authentication as an enhanced technique for authentication on a Smartphone. Through utilising secret-knowledge and keystroke analysis, it is proposed a stronger more robust mechanism will exist. Whilst keystroke analysis using mobile devices have been proven effective in experimental studies, these studies have only utilised the mobile device for capturing samples rather than the more computationally challenging task of performing the actual authentication. Given the limited processing capabilities of mobile devices, this study focuses upon deploying keystroke analysis to a mobile device utilising numerous pattern classifiers. Given the trade-off with computation versus performance, the results demonstrate that the statistical classifiers are the most effective.

Keywords

User authentication, biometrics, keystroke analysis, mobile device

INTRODUCTION

The purpose of authentication is to ensure that access is only given to an authorised person or persons. However, the authentication mechanism itself can vary both in complexity and in cost, and the level of authentication required is inherently tied to the application within which it is deployed. The level of authentication provided by mobile devices to date is arguably commensurate with the level of protection required against misuse, when considering the financial cost of device misuse, due to the limited services and data that can be accessed, versus the cost of implementing an authentication mechanism. However, with the popularity of mobile devices, increasing functionality and access to personally and financially sensitive information, the requirement for additional and/or advanced authentication mechanisms is argued to be essential. Much of this authentication need has come about due to the success of wireless networking technologies that have given devices access to services and information whilst on the move, beyond what is stored within the device itself. As such a secret-knowledge, point-of-entry technique, such as the PIN-based authentication that is currently implemented on all but a few mobile devices, will no longer be sufficient.

As knowledge-based methods might not be appropriate to protect mobile devices by themselves, other types of authentication should be worth looking at. Authentication can be achieved using one of three approaches (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. This category is commonly known as biometrics and it exploits the user's characteristics. Biometrics can be distinguished based upon the features it uses: physiological biometrics identify a user based on the parts of her/his body and behavioural biometrics use the way a user is or interacts (Jain et al., 2004). Keystroke analysis is a type of behavioural biometrics as it authenticates a user based upon her/his typing pattern.

Arguably, the most effective form of authentication would be to use more than one of the aforementioned approaches. Referred to as multi-factor authentication, the approach is able to constructively augment authentication security. The approach proposed in this paper is to use combine secret-knowledge and biometrics. A secret-knowledge based technique will be utilised as usual; however, keystroke analysis will be applied to the

input to provide a second verification. As this approach is based upon the existing authentication approach, no further education of users is required and it can be applied to existing technologies.

Whilst studies have been undertaken looking into the application of keystroke analysis on a mobile device, unfortunately these studies have not specifically addressed the form factor and computational capability of the device – often only using the device to capture samples and then subsequently using desktop computing to analyse the samples. The purpose of this study is to investigate the feasibility of deploying keystroke analysis on a Smartphone.

Section 2 describes the current literature in keystroke analysis, identifying key operational aspects of the system and performance. The paper then proceeds to present the experiment methodology and software development before presenting the results in section 4. The discussion and conclusions are presented in Section 5.

LITERATURE REVIEW

A number of studies have been performed in the area of keystroke analysis since its conception in 1975 (Spillane). Although the studies tend to vary in approach from what keystroke information they utilise to the pattern classification techniques they employ, all have attempted to solve the problem of providing a robust and inexpensive authentication mechanism. Table 1 illustrates a summary of the main research studies performed to date. All, with the exception of Clarke and Furnell (2007), and Ord and Furnell (2000), were based upon classifying users on full keyboards. Ord and Furnell utilised only the numerical part of the keyboard. The paper by Clarke and Furnell (2007) represents the first experimental study performed on mobile devices.

Study	Static/ Dynamic	Keystroke Metrics		Classification Technique	# of Participants	FAR (%)		FRR (%)
		Inter-Key	Hold-Time					
Joyce & Gupta 1990	Static	✓		Statistical	33	0.3		16.4
Leggett et al. 1991	Dynamic	✓		Statistical	36	12.8		11.1
Brown & Rogers 1993	Static	✓	✓	Neural Network	25	0		12.0
Clarke & Furnell 2007	Static	✓		Neural Network	32	5% (Equal Error Rate)		
Napier et al 1995	Dynamic	✓	✓	Statistical	24	3.8% (combined)		
Obaidat & Sadoun 1997	Static	✓	✓	Statistical	15	0.7		1.9
				Neural Network		0		0
Monrose & Rubin 1999	Static	✓		Statistical	63	7.9 (combined)		
Cho et al. 2000	Static	✓	✓	Neural Network	25	0		1
Ord & Furnell 2000	Static	✓		Neural Network	14	9.9		30

Table 1: Review of Literature in Keystroke Analysis

At first glance, it would appear both of the dynamic based studies have performed well against static based approaches, given the more difficult task of classification, however, these results were obtained with users having to type up to a hundred characters before successful authentication. Its applicability to a mobile device in this instance is therefore limited. However, all of the studies have illustrated the potential of the technique, with Obaidat et al. (1997) performing the best with a FAR and FRR of 0% using a neural network classification algorithm. In general, neural network based algorithms can be seen to outperform the more traditional statistical methods, and have become more popular in later studies. Notably, the original idea of keystroke analysis proposed that a person's typing rhythm is distinctive and all the original studies focussed upon the keystroke latency (the time between two successive keystrokes); however, more recent studies have identified the hold time (the time between pressing and releasing a single key) as being as discriminative. However, a study by Karatzouni et al. (2007) identified that the hold-time was not a useful feature for use on a mobile device. The most successful networks implemented a combination of both inter key and hold time measures, illustrating that the use of both measures has a cumulative and constructive effect upon performance.

It is very difficult to directly compare and contrast many of these studies in terms of their verification system and performance, as their method for evaluating (and calculating) the error rates differ depending upon the aim of the study. For example, while some were static-based verifiers, others were dynamic-based with varying

character lengths. However, the initial feasibility study by Clarke and Furnell (2007) does illustrate the applicability of keystroke analysis to a mobile device.

EXPERIMENTAL METHODOLOGY

This study seeks to implement keystroke analysis on a Smartphone. Therefore, a software prototype 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: a simple PIN and 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 Feed-Forward Multi-Layered Perceptron (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.

A group of twenty people participated in the evaluation of the software. In a single session, each participant was asked to enrol by entering their password twenty times and authenticate a further ten times. The forms used for this are illustrated in Figure 1. A SPV C600 Smartphone running Microsoft Windows Mobile 5 was utilised (as illustrated in Figure 2). 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.

The participants were also asked to complete a questionnaire in order to understand their general acceptance of the approach. It assessed their general use of mobile devices, their biometrics knowledge, and the usability and performance of the software.

Enrolment	Authentication
Username: <input type="text"/>	Username: <input type="text"/>
Password type: <input type="text"/>	Password: <input type="text"/>
Password: <input type="text"/>	<input checked="" type="checkbox"/>
<input type="button" value="Menu"/> <input type="button" value="Clear"/>	<input type="button" value="Authenticate"/> <input type="button" value="Close"/>

Figure 1 – Prototype Software



Figure 2 - Evaluation handset: Orange SPV C600

RESULTS

Operational Performance

The evaluation of the pattern classifiers on the Smartphone revealed the importance of the limited processing capacity of devices. Unfortunately, whilst neural network based approaches have traditionally outperformed their statistical counterparts, the study found that the computational requirements of neural networks exceeded the processing capabilities of the device. Table 2 below illustrates the time taken to compute the template and perform verification.

	Enrolment (seconds)	Verification (seconds)
Euclidean	2	~0
Mahalanobis	2	~0
FF MLP – Simple Network	210	10
FF MLP – Complex Network	19 800	20

Table 2: Time taken to complete Enrolment and Verification

Unfortunately, due to the poor performance of the neural network, it was not possible to calculate performance rates for false acceptance (the rate at which impostors are accepted onto the system, FAR) and the false rejection (the rate at which legitimate users are rejected from their system, FRR). The performance for the statistical classifiers based upon entering a PIN and (longer) password are illustrated in Tables 3 and 4.

Strong alphanumeric – Mahalanobis	FRR (%)	FAR (%)	Strong alphanumeric – Euclidean	FRR (%)	FAR (%)
User 2	0	0	User 2	50	0
User 7	0	10	User 7	0	0
User 12	10	10	User 12	30	0
User 19	0	60	User 19	60	0
TOTAL	2.5	20	TOTAL	35	0

Table 3: Performance Results for Password

Simple PIN – Mahalanobis	FRR (%)	FAR (%)	Simple PIN – Euclidean	FRR (%)	FAR (%)
User 1	0	0	User 1	0	10
User 3	0	70	User 3	0	40
User 4	70	80	User 4	20	80
User 5	20	80	User 5	50	40
User 6	0	100	User 6	0	90
User 8	0	90	User 8	10	50
User 9	40	20	User 9	40	40
User 10	50	40	User 10	10	100
User 11	30	0	User 11	10	0
User 13	50	0	User 13	80	0
User 14	10	50	User 14	0	100
User 15	20	20	User 15	0	60
User 16	20	70	User 16	0	100
User 17	0	100	User 17	0	60
User 18	20	60	User 18	20	80
User 20	0	70	User 20	0	70
TOTAL	20.63	53.13	TOTAL	15	57.5

Table 4: Performance Results for PIN

From an analysis of the two statistical classifiers it appears there is little difference in the actual performance obtained using either the PIN or password. However, the results do clearly demonstrate that the performance of the classifiers on the password is considerably stronger than the PIN. From prior literature, this was expected due to the increased number of keystroke latencies with which the classifier can use – therefore arguably more discriminative information that is contained in longer feature vectors. Whilst, these results are produced from a relatively short population of participants, it would suggest the use of a short PIN would be ineffective for use within keystroke analysis. However, ensuring users use a longer PIN or stronger alphanumeric password would enable keystroke analysis to be applied.

Usability Assessment

The second aspect of the evaluation, the questionnaire, investigated the participants' thoughts about their knowledge and usability of the software. To begin, they responded to general questions about their mobile device use. Interestingly, 7 out of the 20 participants do not use any security measure on their handset and fifteen users think that their device information is sensitive. Moreover, 5 out of the 7 participants who did not use any security feature think their information is sensitive. When asked to consider which authentication approaches they would use on a mobile device, fingerprint based solutions were the most popular (as illustrated in Figure 3). This is arguably expected, as prior surveys have always suggested users are more willing to adopt technologies they are aware of.

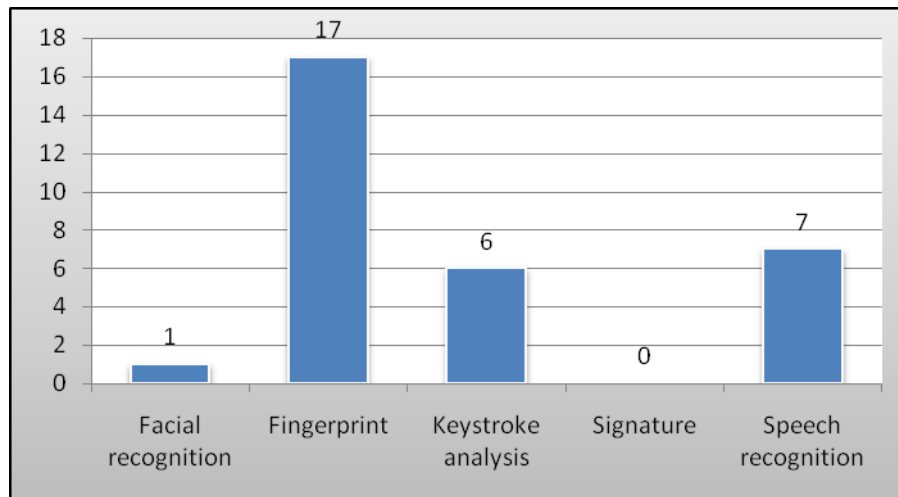


Figure 3: Users preference towards Biometric technologies

Asked to assess whether they thought the software was simple to use, 19 users thought that the software is easy to use; however, half of them found the enrolment time consuming. The participants justified the length of the process by the number of samples that needed to be entered. Effectively, they estimated that 20 samples was 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.

Discussion

Time seems to be a significant problem when implementing keystroke analysis on a mobile device – whether it is the time taken to undertake enrolment or the time taken to compute the biometric template. It therefore argued that any practical implementation of the system must take careful consideration of the usability of the approach; ensuring users experience a short enrolment and timely response in authentication.

In order to remove the necessity of providing 20 samples for enrolment, it is suggested the system could included a two-part process, where the user simply provides the password once in the first instance. The user would then login to their phone in the normal manner (for instance daily) – each time keystroke samples being acquired. Once sufficient samples have been acquired, keystroke analysis would then be applied to the login process. Whilst the device will only be protected using a single-factor technique in the first instance, the ability to remove the troublesome enrolment process, in addition to arguably obtaining more representative samples

from the user are key advantages. Once the template has been created, the full two-factor approach can be applied.

Unfortunately, the applicability of implementing neural networks on a Smartphone is poor, with algorithms at present too computationally demanding for processors. However, given the rapidly evolving nature of mobile devices and their ever-increasing processor speeds and capacities, it is envisaged this will not remain a problem. Given prior literature has clearly illustrated the performance gains to be achieved using these algorithms, it is suggested a flexible approach be taken when implementing keystroke analysis. Through implementing an approach that includes multiple classifiers, the software would be in a position to assess which of the algorithms would be most suitable given the processing and memory capacities of individual devices.

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 one third 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. Overall, it seems encouraging that they are willing to use new security solutions, with 18 willing to use this technique and all of them considering that the approach improved the level of security. 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.

CONCLUSIONS AND FUTURE WORK

This study has showed that keystroke analysis could be implementable on a mobile handset technically and that users would be willing to adopt such an approach. The statistical classifiers demonstrated low processing requirements that can be used on a real device, with timely responses in both the template generation and verification of samples. However, the results have shown the importance of the type of input used; with 4-digit PIN based approaches being too short in practice to use.

Future work will seek to investigate the optimisation of neural network based approaches and develop techniques for assessing processor performance so that an appropriate classifier can be selected on an individual basis. The authors will also look to integrate the solution into the Microsoft Windows Mobile security architecture. 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. This will provide a completed solution and enable a more thorough evaluation by participants – as we would be in a position to provide the software as a download that would integrate into any Windows Mobile based device.

REFERENCES

- Brown, M., Rogers, J. (1993). "User Identification via Keystroke Characteristics of Typed Names using Neural Networks". *International Journal of Man-Machine Studies*, vol. 39, pp. 999-1014
- 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. and Furnell, S.M. (2007) 'Authenticating mobile phone users using keystroke analysis' *International Journal of Information Security*, 6 (1): 1-14.
- 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.
- Joyce R., Gupta, G. (1990). Identity Authentication Based on Keystroke Latencies. *Communications of the ACM*, vol. 39; pp 168-176.
- Karatzouni S, Clarke NL (2007): "Keystroke Analysis for Thumb-based Keyboards on Mobile Devices", *Proceedings of the 22nd IFIP International Information Security Conference (IFIP SEC 2007)*, Sandton, South Africa, 14-16 May, pp. 253-263
- Leggett, J., Williams, G., Usnick, M. (1991). "Dynamic Identity Verification via Keystroke Characteristics". *International Journal of Man-Machine Studies*.

- Monrose, R., Rubin, A. (1999). "Keystroke Dynamics as a Biometric for Authentication". *Future Generation Computer Systems*, 16(4) pp 351-359.
- Napier, R., Lavery, W., Mahar, D., Henderson, R., Hiron, M., Wagner, M. 1995. "Keyboard User Verification: Toward an Accurate, Efficient and Ecological Valid Algorithm". *International Journal of Human-Computer Studies*, vol. 43, pp213-222
- Obaidat, M. S., Sadoun, B. (1997). "Verification of Computer User Using Keystroke Dynamics". *IEEE Transactions on Systems, Man and Cybernetics – Part B: Cybernetics*, Vol. 27, No.2.
- Ord, T., Furnell, S. (2000). "User Authentication for Keypad-Based Devices using Keystroke Analysis". MSc Thesis, University of Plymouth, UK.
- Spillane, R. (1975). "Keyboard apparatus for personal identification". *IBM Technical Disclosure Bulletin*, 17, 3346.
- Wood, H.M. (1977) 'The use of passwords for controlled access to computer resources', *National Bureau of Standards*, Special Publication 500-9.

COPYRIGHT

A. Buchoux and N.L. Clarke ©2008. The author/s assign Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. The authors also grant a non-exclusive license to ECU to publish this document in full in the Conference Proceedings. Any other usage is prohibited without the express permission of the authors.