Invisible, Passive, Continuous and Multimodal Authentication

Karen Renaud and Heather Crawford

School of Computing Science
Sir Alwyn Williams Building
University of Glasgow
Glasgow UK, G12 8RZ
karen@dcs.gla.ac.uk, hcrawford@fit.edu

Abstract. Authentication, as traditionally achieved by means of a shared secret, is effortful and deliberate. Frequent and repeated authentication easily becomes a hurdle, an annoyance and a burden. This state of affairs needs to be addressed, and one of the ways of doing this is by moving towards automating the process as much as possible, and reducing the associated effort — ie. reducing its visibility. A shared secret clearly does not have the flexibility to support this, and we need therefore to consider using biometrics. Biometrics are a well-established authentication method. Physiological biometrics require a biometric reader and explicit action by the user. Furthermore, there are always a minority of users who cannot have a particular biometric measured. For example elderly women often lose their fingerprints, and iris biometrics don't work for people with particular eye conditions.Behavioural biometrics, however, can be collected without the user having to take deliberate action. Hence there is a strong possibility that these biometrics could deliver the invisible and automatic authentication we are striving towards. One big advantage of these biometrics is that, since there is no reader, it is simple to utilise a number of different biometrics, and to combine these to authenticate the user. If one biometric fails the others can still perform authentication.

Here we propose using patterns such as keystroke dynamics, use patterns, and voice analysis techniques to create a multimodal biometric authentication mechanism. These *behavioural* biometrics take advantage of tasks that the user already performs thereby reducing the need for explicit authentication by more traditional means. In this way, the user is relieved of the burdens of constantly authenticating to multiple applications and devices.

1 Introduction

It is clear that the username-password "identity" combination, while perfectly satisfactory from a purely technical security perspective, is inherently flawed when used by fallible humans. Passwords are forgotten, shared and reused on multiple devices and applications. The policies implemented to strengthen passwords, such as requiring sufficient length or strength and changing the password

R. Murray-Smith (Ed.): MSSP 2010, LNCS 8045, pp. 34–41, 2014.

frequently, may not increase the security level since users simply find other ways of coping, such as writing the passwords down. Furthermore, the password, as a concept, does not authenticate the user; it authenticates an identifier. Someone else might be holding that identity, and the system errs in assuming that the verified identity authenticates the legal owner thereof. Clearly this mechanism is too weak to control access to many systems but, in the absence of a viable alternative, the flawed password prevails.

The type of security today's computers require, with their almost unlimited access to personal and private information, must go beyond secret knowledge and uniquely authenticate a particular *person*. We must be able to prove, with far more confidence than the password affords, that a person is who they claim to be, before granting them access to a restricted resource.

Authentication is traditionally achieved by using one of three classes of authenticator: something you *have*, something you *know*, or something you *are* [20, p. 29].

- *something you have*: the user is in possession of a physical device or token that aids in identification. The debit card associated with a particular bank account is an example of a token.
- *something you know*: requires a user to prove knowledge of a particular secret. Secret knowledge techniques such as knowledge of a password or PIN are examples of something you know.
- *something you are*: concerned with measuring a person's physical attributes as a unique identifier, and referred to as biometrics. Examples include fingerprints, retinal scans, and facial recognition. Biometric is "the science of recognizing an individual based on her physiological or behavioral traits." [18]. Interestingly, this definition also includes *behavioral* traits, which include typing style, device use patterns, and gait analysis, to name just a few. Unlike physical biometrics, which require the user to submit to their capture, behavioral biometrics can be captured while the user goes about their everyday tasks. This reduces reliance on the user to authenticate correctly and also allows authentication to take place invisibly. According to a 2004 study, users prefer biometrics to passwords since they believe biometrics would provide an increased level of security [16].

2 Motivation

In addition to increasing the need for more reliable access control and authentication mechanisms, the new generation of mobile computing devices has also increased the user's memory and cognitive load due to different usage paradigms imposed by these devices. Great care needs to be taken when deciding on an authentication mechanism for such devices. The user's main goal is to perform some task, such as checking their bank balance or calling a friend. Authenticating themlselves is extraneous, and it makes no sense to impose a complicated authentication onto them.

Authentication could benefit from being a "black box" – the user is aware of its operation and has confidence in the fact that they are accessing a secured device or action, but has little idea how the minitiae of the authentication procedure is being achieved. In order for authentication to be achieved in a black box fashion, it has to be designed with fault tolerance in mind. This needs to be achoeved by means of redundancy. The user should never be prevented from accessing needed resources if there is a failure in one component of the authentication mechanism. The mechanism should be able to function recover from partial failures so as to maintain its rationale of being as invisible as possible. Users should be freed to concentrate on their primary tasks, without being required to explicitly prove their identity from time to time.

The remainder of this paper examines three behavioral biometrics: keystroke dynamics, voice analysis, and use patterns. It is envisaged that these will be combined to achieve the invisible multimodal authentication that will facilitate a black box approach.

3 Multimodal Biometrics

A biometric identification system is called *multimodal* if it combines two or more biometric identifiers in order to authenticate a user. For example, physiological biometric systems can use a combination of, say, fingerprints and retinal scans to improve the probability of correctly identifying a user. The purpose of combining more than one biometric is to reduce the possibility of errors (either False Accept, where an unauthorized user is granted access, or False Reject, where an authorized user is denied access) and to reduce the dependence on a single identifier. Consideration must be given to how the biometrics are combined. The two possibilities are to combine each of the patterns into a single pattern, and make a decision based on that pattern, or to make a decision based on each pattern collected, and then combine the individual decisions into a final determination. Behavioral biometrics can also be combined into multimodal biometrics. This section examines three possible behavioral biometrics that are candidates for combination: keystroke dynamics, voice analysis, and use patterns.

3.1 Keystroke Dynamics

Keystroke dynamics attempts to uniquely identify a device user based on their typing patterns, either by requiring them to type a specific phrase or by simply sampling the user's typing patterns while they use applications that require keyboard input. Interest in keystroke dynamics as a potential distinguishing characteristic has a long history. It was applied to Morse code operators - clever listeners could distinguish one operator from another by the operator's *fist*, which is the distinctive pattern and speed of the dots and dashes transmitted. Keystroke dynamics on computers was first suggested as a behavioral biometric by Spillane in 1975 [21]. Since then, an extensive amount of research has been performed in this area. Studies have examined its viability as an authenticator on both mobile

devices [5,8,19] and desktop computers [1,10,15]. Early attempts used statistical classifiers to determine whether a person's keystroke patterns matched a previously stored pattern, but the state of the art is to now use neural networks, since their use has been shown to reduce the number of characters required to identify a user [6].

On its own, keystroke dynamics is not expected to be enough to uniquely identify an individual, although there is sufficient information to allow identity verification [13]. Its strength is that typing is something that most users do when interacting with a computing device, and therefore collecting typing characteristics can be undertaken by taking advantage of the users' current tasks. Although keystroke dynamics is not discriminatory by itself, it lowers the likelihood of accepting unauthenticated users. When combined with other similar biometrics, the data presented with keystroke dynamics is expected to provide enough information to uniquely identify a particular user.

3.2 Voice Analysis

Voice analysis compares samples of a person's voice to a pattern from the known authorized user. While voice recognition is a heavily researched field, the amount and quality of available research has declined since 2001. It has been found to be an area of limited potential because a person's voice alone is not considered unique enough to be the basis of an authentication mechanism [3]. If the main goal of the voice analysis is to *identify* a given person, the research supports this method, although there are still limitations. The quality of the microphone as well as distortions due to background noise can negatively affect the standard of the voice patterns gathered.

Despite this negative result, some research has been done on using speech as an authentication mechanism, often in conjunction with another biometric to form a multimodal biometric system. Iwano *et al.* combined speech analysis with ear images to create a multimodal biometric system, but the speech analysis had significant Equal Error Rate (EER) values (around 40% with a low Signal to Noise ratio [12]. The results of combining speech analysis with ear images was more promising; the error rates dropped by about 75%, although were still far to high to be used as a biometric. Voice patterns were matched with facial recognition to create a multimodal system designed by Brunelli and Falavigna in 1995 [4], although the error rates for voice analysis alone were quite high at 14%. The BIOMET system developed by Garcia-Salicetti *et al.* uses five identifiers including voice patterns to distinguish one person from another [9]. The purpose for using such a large number of identifiers was to offset the failings of each identifiers with the strengths of the others. None of the systems studied so far has a low enough error rate for the voice analysis section alone to uniquely identify individuals.

Voice analysis as a possible authenticator need not be discarded completely, however. Research has been performed in the area of *conversational* voice analysis, where the patterns of a person's natural way of speaking (i.e., speed, pronounciation, word repetition) are used to identify a person [17]. In some cases,

it is the role the person plays in a conversation (say, boss and employee or interviewer and interviewee) that was studied rather than identifying the actual person [23]. This part of the voice analysis module is promising, and is likely to provide a suitable level of certainty that a person is who they claim to be. When combined with other behavioral biometrics, conversational analysis becomes a promising possibility for passive authentication.

3.3 Use Patterns

Use patterns involves collecting information on how the user interacts with a computing device (i.e., a laptop, desktop computer, or mobile device) and using the uniqueness in these patterns as a biometric identifier. Examples include who the user calls or sends text messages to, and how often, web sites visited, applications that are loaded, and what type of music is played and with what frequency. These uses of a device provide a rich source of information about who is using the device since it is unlikely that any two people use a device in exactly the same manner.

Use patterns have generated some interest in the area of behavioral biometrics. Clarke *et al.* mentioned "service utilization" as a possible behavioral biometric in their study of users' attitudes regarding authentication on mobile devices, but did not attempt to use it in a working system [7]. While it is clear that there is some identifying information to be found in tracking a person's device use, it has not been a well-researched area, particularly in the mobile device field. When combined with other authenticators such as voice analysis and keystroke dynamics, it is hoped that it will provide a method of further reducing error rates.

4 Pattern Classification

Biometric systems, both physiological and behavioral, use pattern classification methods to compare a known sample to a gathered sample. The two major fields of pattern classification that are used in biometrics research are statistical classifiers and neural networks. In practice, neural networks are often considered a sub-type of statistical classifiers [2, p. 8]. Statistical pattern recognition algorithms use statistical information about each biometric sample in order to classify them into groups. The patterns are feature sets that group together defining points (i.e., measurements) in the original signal in order to create a symbolic representation of that signal. Examples of statistical pattern classifiers are Bayesian filters, naive Bayes classifiers, and the k-Nearest Neighbor algorithm. Neural networks are an extension of statistical pattern recognition since they follow the same sorts of rules, but have improved upon them with the improvement in computing power and resources. The use of neural networks has reduced the length of the string required in order to authenticate a user via keystroke dynamics. [6], which makes authenticating using a short character string viable. Despite the long research history of statistical methods, they

have been found to produce higher error rates in keystroke dynamics research, when compared to neural networks [5]. However, there are always tradeoffs when selecting an algorithm to use in a computing environment; in this case, neural networks require a large training set in order to correctly classify patterns, they must be re-trained if a new user is added to the network, and they are computationally and memory-intensive pattern classification methods [5,14].

In addition to the practical concerns of what type of pattern classifier to use, consideration must also be given to the results of such comparisons. As with all biometric systems, samples of each person's voice, keystroke patterns, and use patterns must be made available for comparison and testing purposes, but there must also exist a large set of "world view" patterns for each of the three biometrics. The reason for this is twofold: first, the non-authenticated user patterns can be used to test whether the module in question reduces the confidence level in the presence of a non-matching pattern. The second reason is somewhat more important. In order to show that a particular pattern type is a good candidate for a behavioral biometric, it must be shown that the user's pattern is distinct enough from a representation of other users' patterns – the so-called world view. Therefore, not only must the chosen biometric identifier be unique enough for comparisons, it must also have a large corpus of non-authenticated patterns to make up the world view. Such corpora are widely available for voice patterns [11,22], but are not necessarily available for use patterns or keystroke information on a mobile device. Such corpora must be created in order to provide proof that the chosen biometric provides the distinctiveness required for authentication purposes.

5 Conclusion

Behavioral biometrics have strong potential as a passive authentication mechanism. Careful thought must be given to how uniquely identifying each biometric is, and whether the biometric pattern can meaningfully be combined with others to constitute a multimodal identifier. Such identifiers improve the system by providing additional certainty that the user is who they claim to be. Such redundancy can be seen in many mature and workable systems, and provides a measure of fault tolerance that is essential in biometric authentication systems. Consideration must also be given to showing that a particular biometric can be uniquely identified from a world view of other such patterns, in order to show that the biometric will match its owner's pattern, and no other, with a reasonable degree of certainty. These considerations will serve to guide the research process and their existence provides strong support for future research in the area of behavioural biometrics as an authentication method.

This mechanism is not without its concerns. There are privacy concerns related to the use of behavioral biometrics since the type of data gathered is from user's private emails, text messages, telephone calls, and physical location. This research will use anonymising techniques so that as much personal detail as possible is removed, although removal of all data will be impossible.

References

1. Ahmed, A.A.E., Traore, I., Almulhem, A.: Digital Fingerprinting Based on Keystroke Dynamics. In: Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurance (HAISA 2008), Plymouth, UK, pp. 94–104 (July 2008)
2. Bishop, C.M.: Neural Networks for Pattern Recognition. Oxford University Press (1995)
3. Bonastre, J.-F., Bimbot, F., Boe, L.-J., Cambell, J.P., Reynolds, D.A., Magrin-Chagnolleau, I.: Person Authentication by Voice: A Need for Caution. In: Proceedings of Eurospeech 2003 (2003)
4. Brunelli, R., Falavigna, D.: Person Identification Using Multiple Cues. IEEE Transactions on Pattern Analysis and Machine Intelligence 17(10), 955–966 (1995)
5. Buchoux, A., Clarke, N.L.: Deployment of Keystroke Analysis on a Smartphone. In: Proceedings of the 6th Australian Information Security Management Conference, Perth, Western Australia, pp. 40–47. SECAU - Security Research Centre (2008)
6. Cho, S., Han, C., Han, D.H., Kim, H.-I.: Web based Keystroke Dynamics Identity Verification Using Neural Network. Journal of Organizational Computing and Electronic Commerce 10(4), 295–307 (2000)
7. Clarke, N.L., Furnell, S.M., Reynolds, P.L.: Biometric Authentication for Mobile Devices. In: Proceedings of the 3rd Australian Information Warfare and Security Conference 2002, pp. 61–69 (2002)
8. Clarke, N.L., Furnell, S.M.: Authenticating Mobile Phone Users Using Keystroke Analysis. International Journal of Information Security 6(1), 1–14 (2007)
9. Garcia-Salicetti, S., Beumier, C., Chollet, G., Dorizzi, B., Leroux les Jardins, J., Lunter, J., Ni, Y., Petrovska-Delacretaz, D.: BIOMET: A Multimodal Person Authentication Database Including Face, Voice, Fingerprint, Hand and Signature Modalities. In: Kittler, J., Nixon, M.S. (eds.) AVBPA 2003. LNCS, vol. 2688, pp. 845–853. Springer, Heidelberg (2003)
10. Gunetti, D., Picardi, C.: Keystroke Analysis of Free Text. ACM Transactions on Information and System Security 8(3), 312–347 (2005)
11. Hirschman, L.: Multi-Site Data Collection for a Spoken Language Corpus. In: Proceedings of the Workshop on Speech and Natural Language, pp. 7–14. ACM (1992)
12. Iwano, K., Hirose, T., Kamibayashi, E., Furui, S.: Audio-Visual Person Authentication Using Speech and Ear Images. In: Proceedings of Workshop on Multimodal User Authentication, pp. 85–90 (2003)
13. Jain, A.K., Ross, A., Prabhakar, S.: An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology 14(1), 4–20 (2004)
14. Karatzouni, S., Clarke, N.: Keystroke Analysis for Thumb-based Keyboards on Mobile Devices. In: Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R. (eds.) New Approaches for Security, Privacy and Trust in Complex Environments. IFIP, vol. 232, pp. 253–263. Springer, Boston (2007)
15. Obaidat, M.S., Sadoun, B.: Verification of Computer Users Using Keystroke Dynamics. IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics 27(2), 261–269 (1997)
16. Price Waterhouse Coopers. Information security breaches survey 2004. Technical report, Department of Trade and Industry (2004)
17. Psathas, G.: Conversation Analysis: The Study of Talk-in-Interaction. Sage Publications (1995)

18. Ross, A., Jain, A.K.: Multimodal Biometrics: An Overview. In: Proceedings of the 12th European Signal Processing Conference (EUSIPCO), pp. 1221–1224 (September 2004)
19. Saevanee, H., Bhattarakosol, P.: Authenticating User Using Keystroke Dynamics and Finger Pressure. In: Proceedings of the 6th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA, pp. 1–2. IEEE (2009)
20. Smith, R.E.: Authentication: From Passwords to Public Keys. Addison-Wesley (2002)
21. Spillane, R.: Keyboard Apparatus for Personal Identification. Technical Report 17, IBM Technical Disclosure Bulletin (1975)
22. Taussig, K., Bernstein, J.: Macrophone: An American English Telephone Speech Corpus. In: Proceedings of the Workshop on Human Language Technology, Plainsboro, NJ, USA, pp. 27–30. ACM (1994)
23. Vinciarelli, A.: Speakers Role Recognition in Multiparty Audio Recordings Using Social Network Analysis and Duration Distribution Meeting. IEEE Transactions on Multimedia 9(6), 1215–1226 (2007)