Biometric Daemons: Authentication via electronic pets

Pam Briggs
PaCT Lab, Northumbria University
Northumberland Building
Newcastle upon Tyne, NE1 8ST, UK
p.briggs@northumbria.ac.uk

Patrick Olivier
Newcastle University
Computing Science, Culture Lab, King's Walk
Newcastle-Upon-Tyne, NE1 7RU, UK
p.l.olivier@ncl.ac.uk

Abstract

A well-known security and identification problem involves the creation of secure but usable identification and authentication tools that the user is fully motivated to adopt. We describe an innovative solution to this problem: The Biometric Daemon, which takes its inspiration from two sources. It is firstly conceived as a biometric device which is initially imprinted with the fixed biometric properties of its owner, and is then regularly updated with the fluid biometric properties of its owner. However it also acts as an electronic pet which (i) part-shares identity with its owner, (ii) needs nurturing and (iii) effectively dies when separated from its owner for any length of time. Our proposal was inspired by the literary daemons described by Philip Pullman. Our Biometric Daemon synthesizes the properties of biometric token and daemon and we argue that it offers the basis for secure, usable and engaging identification and authentication.

1. The problem

The fundamental security problem involves controlling access to certain information, functions or areas – keeping certain people in and others out. Typically this problem is framed in terms of processes of identification (where an individual is asked who he or she is and responds with an identification token such as a name, email address or account number) and authentication (where an individual will be asked to demonstrate that they are the person they claim to be) [14]. Authentication can involve a variety of methods, but none are currently problem-free. Firstly, an individual may authenticate their identity by drawing upon some memory, typically recalling a mother's maiden name, a place of birth or favorite town or alternatively, recognizing a familiar image embedded in a set of diverse images. Such systems are simple in concept, but these mechanisms create a problem commonly experienced by most computer users – memory overload. Many people cope with memory overload by relying on one or two obvious passwords – the name of a partner or the date of birth of a child – and indeed these 'weak passwords' do ease the overload problem, but they then fail to offer adequate levels of protection. Reliance on names, for example, means that most codes can be easily broken. Conversely, 'strong passwords' [16] may offer higher security levels but are very difficult for an individual to remember

A second means of authentication involves the use of some possession (e.g. a credit card or library card) to validate identity. Physical tokens such as credit cards or security tags will allow individuals access to services or allow entry into a secure area, but unfortunately these are easily stolen or copied. The usual solution is to combine the token with some other authentication mechanism (memory or biometric verification) – thus ensuring that a stolen token used in isolation will be useless. However any individual who uses a pin number to validate a credit or debit card will be aware of the ease with which confidential information is given away to 'shoulder surfers'. In addition, various fraudulent devices are available that can capture both the information present on a card and the accompanying pin number (e.g. a skimmer used in conjunction with a discreet camera) thus rendering such security methods vulnerable to attack [5]. Finally, authentication may be achieved by recording personal (physiological or behavioral) attributes of the owner and using these biometric markers as a means of authenticating identity [2]. Physiological biometrics are perhaps the best known. These consist of unique and distinctive properties of the body and include fingerprints, vein, iris and retina patterns, face hand or finger geometry or voice patterns. However, behavioral biometrics such as mouse, keystroke or signature dynamics have also been shown to be reliable as they too involve unique patterns that can be captured and subsequently identified [8].

Yet biometrics are also fallible authentication mechanisms. Fingerprints can be sliced off or (rather less gruesomely) recreated in plastic. Voices or faces can be reproduced. Moreover, biometrics are sometimes associated with usability and acceptability problems. Enrollment can be quite a sensitive and time consuming process, often requiring a calm, controlled environment and subsequent validation can be intrusive (as, for example, with retinal or iris scanning). In addition, biometrics, perhaps more than any other authentication mechanism, carry a social agenda. Devices that are created to recognize the fingerprints of the masses may have difficulty with the fingerprints of the few. Thus older adults, known to have thin skin with little elasticity, find it difficult to successfully enroll and verify fingerprints across a range of systems [11]. Finally, there is a strong political agenda in relation to biometrics. Users express concern that some fundamental aspect of themselves is stored in a database and worry about database safety. Such fears have been heightened recently in the UK, following the well-publicized loss of two computer discs containing 25 million personal data records [15].

When these problems are taken overall, it is, perhaps, not surprising that one of the key issues for any authentication system is the simple one of adequately motivating users [1]. In the long-term, it is probably not enough to simply keep users informed about existing and potential threats or bombard them with reminders to act in a secure fashion. We know that we should protect our pin from prying eyes and choose tricky passwords, but such security practices are often tedious or troublesome. We might accept that a biometric solution frees up memory, but we feel uncomfortable as we line up to offer our fingerprints to US immigration. Nor are we alone in recognizing that security comes at a price [3]. But might we be able to create a security tool that overcomes some of these obstacles – that is both engaging and fun to use, but that also offers the highest standards of user protection?

2. A solution

Our solution is to create a tool that is uniquely personalized to the end user. In doing so, we recognize that one of the most prevalent trends in human-computer interaction is the creation of objects and systems that offer the potential for deep personal significance. Our solution combines the relative rigor of biometric authentication with the delights of an electronic pet – a metaphor that naturally targets personalization. We propose, simply, that identification and authentication can be combined in one usable token, provided that that token

'lives' and develops a unique relationship with its owner akin to that between owner and pet. In effect, a token that pines and ultimately dies when separated from its owner would be the ultimate security tool. Our concept, then, is of an entity that acts in its simplest mode like a credit card and pet combined. Or more specifically, a credit card and daemon (as described by Philip Pullman [13] – i.e. a pet that shares identity with its owner and that dies if separated from its owner for any length of time. This solution is explained in more detail below.

Contemporary design is not about static objects, but about objects that have adaptive capability. In our case we are talking about a process in which, over time, object can uniquely recognize and respond to owner and is in turn trusted to do more significant and secure work. Of course the starting point is also important. Not all animals take time to build up a relationship. Chicks, for example, have a 'sensitive period' between ten and twenty hours after hatching in which they will learn to recognize their mother (as the closest moving object during this time) and will bond with her in a process known as 'imprinting', following her thereafter. This imprinting process is a key mechanism for ensuring the safety of the newborn and ensuring it is reared in an appropriate context. In the Philip Pullman 'Northern Lights' (published in America as 'The Golden Compass') we are introduced to the concept of the daemon. Daemons have a number of interesting properties. They are animal in form, but share an identity with their owner – and exhibit an intimacy based upon seamless communication of a shared emotional state. Any separation between daemon and owner will result in the death of the daemon.

If we move now, to the concept of a biometric daemon, we can see that there are unique advantages, within the security domain, to an object that relies on the co-presence of its owner for its very survival. Up until now, with standard security tokens, this co-presence has been signaled by the owner presenting the token with some deeply personalized information (a personal memory), but our daemon requires no such validation as its own health status is a direct indicator of the co-presence of the appropriate owner. A biometric daemon, can therefore be a token that can be trusted in isolation provided that it signals both health and happiness, has the latter signals directly imply that it's owner is co-present, or at least that it has been very recently reassured (of which more later).

3. Two processes: Imprinting & nurturing

We propose that our biometric daemon must initially go through a period of imprinting (when it becomes exposed to the identify information of an individual but simultaneously bonds to that individual). But we also believe that the daemon should subsequently be nurtured in a process involving touch, conversation and familiar but idiosyncratic movements (either deliberate and playful such as rocking, or incidental as when carried in a pocket). The design of such nurturing interactions may take inspiration from existing virtual or robotic pets with the Tamagotchi being perhaps one of the best known examples.

Firstly, let's explore the initial imprinting process in more detail. Imagine that an individual has been given a date to go to the 'clinic' to collect a daemon. It's an exciting day, as this user-daemon partnership will continue for years to come. After a ritual (in a secure environment) in which the user commits identity information to the daemon, he or she then lifts the neophyte from its protective shell and, holding it in the palm of the hand, strokes it gently. These activities provide the necessary information (e.g. palmprint or fingerprint) to bring the daemon to life and to ensure that it is loyal to this person alone. Naturally this imprinting process must be completed with an appropriate understanding of biometrics requirements. Fingerprint-based enrollment, for example, may require several attempts in order to yield a high quality template – but these attempts can be made seamlessly and naturally in the process of holding and stroking the daemon in order to coax it into life. Now let us consider the active life of the daemon. We know that authentication and identification can be achieved through an understanding of both fixed (e.g. fingerprint) and fluid (e.g. voice pattern) attributes which means that biometric information can be both acquired and learned over time. While fixed biometrics may lend themselves to the imprinting process described above, the more fluid biometrics would lend themselves to a nurturing process which could be either incidental (when the daemon may come to learn the sound of its owner's voice or a particular gait) or could be deliberate.

Incidental nurturing means that a daemon comes to recognize the stable elements of its environment and is subsequently reassured by them. These elements could involve behavioural biometrics, such as the acceleration profile of the daemon as it is carried about (i.e. recognition of the owner's familiar gait) or the acoustic qualities of its environment (i.e. quiet and familiar voices are reassuring). The elements could go beyond personal biometrics, however. For example, the daemon could use GPS to determine spatiotemporal contexts (i.e. is this a familiar place, and a familiar time to be in this place) or might come to recognize other people in an environment through the identity of personal area networks (i.e. visible Bluetooth-enabled and other wireless devices). Thus incidental nurturing can take place as an accretion of familiar signals in the daemon's immediate environment.

By contrast deliberate nurturing is a process whereby an owner seeks to reassure their daemon through a well established, but personal, act of reassurance. This might be envisaged a process whereby an owner regularly plays with his or her daemon, teaching it secret idiosyncratic games involving movement, words or sounds. The acts of deliberate reassurance are incorporated as useful additions to physical biometric identification since the unique and intimate nature of these acts serves not only to reassure the daemon but to reinforce the emotional connection between the owner and the daemon. This deliberate nurturing process is, therefore, not unlike the process of playing with a pet. By the combination of these nurturing processes, both active (deliberate) and passive (incidental) the daemon is reassured and continues to thrive. Without this kind of continuous authentication, the daemon becomes distresses, pines (effectively refusing to work – see below) and eventually dies.

We argue that the two processes of incidental and deliberate nurturing are technically feasible since they can be seen as plausible extensions of a range of behavioral and physiological biometrics already documented. These include voice [10] [6], gait [4] [9] and physical action (e.g. keystrokes [12]). Note, too, that this process of adaptive continuous authentication is expressed in simple terms here, but has huge potential. For example, a daemon equipped with location awareness can come to know and understand the places (and people) that are important to an owner and could, potentially, need more than the usual amount of reassurance if they are taken outside their geographic comfort zone. Similarly, the daemon can understand other security relevant patterns of behavior and can seek additional reassurance if, for example, a purchase requires an unusually large amount of money or if highly sensitive personal information is requested.

4. The Daemon at work

This pet has a job to do and we can envisage this job in two ways. Firstly, and most simply, the daemon can act as an authentication token – an elaborate identity card –

capable of signaling to a nearby device that the owner is co-present. In this signaling system the device simply needs to know that the daemon is in a happy state (achievable only when it has been given sufficient reassurance to be so). In conventional settings, such as at an ATM, this reassurance will in part come from the biometric signals of the owner, but could also include other familiar signals inherent in the transaction itself (e.g. using a familiar ATM in a known location could be more reassuring than using a novel ATM). The relationship between the daemon's emotional state and the security contexts they encounter would soon become transparent to owners. Thus, owners might prepare and reassure their daemons not only at the point of a transaction, but in anticipation of an authentication challenge.

In this way, then, the daemon could come to act as a trust agent [7] helping its owner make decisions about who to trust with access, information, or data. In suggesting this, we are recognizing that the security tasks of the future are likely to be much more complex than the tasks of the present. In a ubiquitous computing environment, for example, an individual may be bombarded with requests authorizing the release of personal data but may not be able to make individual decisions about the risks inherent in each request. If we imbue our daemon with the capacity to monitor not only location or transaction information (as above) but also to monitor relationships between enquiring agents then we can see how our daemon could come to play a role as a kind of personal historian, maintaining and evaluating exchanges and ultimately assigning trust values to different enquirers. In this way, the exchanges between owner and daemon are built up into a profound personal history which can be used to set the levels of reassurance required in any future transactions.

5. Co-evolution & delegation

It is possible to introduce two further processes into the owner-daemon relationship, although we acknowledge that these are highly speculative and their value open to further investigation. We have described nurturing as a longer-term process designed to introduce the daemon to behavioral biometrics, but another process, of co-evolution may take place over much longer timescales. For example, in the case of domestic dogs, co-evolution over many generations has led to a number of behavioral traits, such as maintaining eye contact, that are beneficial to the human-animal relationship but not apparent in wild dogs or other animals (where eye contact is a component of confrontation). Over longer intervals of time, potentially even generations, the dae-

mons will evolve both better biometric recognition and behaviors that are appropriate to the actions, activities and security requirements of owners. As with pets, such traits might diverge at a "breed" level. Different breeds will possess different levels of independence, sensitivities, forms and behavioral profiles, and be selected by users on the basis of these breed traits. Of course, effecting a process through which such traits would emerge arises requires a process of selection which presupposes that the development of one generation of daemon's impacts on the configuration of the next generation.

Delegation would be a process by which one would reassure one's daemon in the presence of another individual (or daemon) in order that it eventually reaches a temporary state of attachment to another. An example might involve passing the daemon from user to delegate repeatedly while playing some kind of vocal game. A temporary relationship is created between the core biometric profile of the user and the biometric signature of a new host. In this fashion a daemon could be given over into the care of another person and would remain in an active or healthy state for a short while in order for that person to, say, access funds or authorize payments for an individual while they spend some time in hospital

6. Why have Biometric Daemon?

Our daemon can transform the user experience of security by making it both more enjoyable and also more meaningful. In summary, our biometric daemon offers the following important advantages:

(i) It has face-validity as a high-level security system. The mental model of the protective dog that only responds to its owner works well here. We therefore tap into a common sense, palpable understanding of security that is reinforced when the user sees the daemon exhibiting signs of distress when handled by others but regaining normal function when returned to the owner. Such an intuitive grasp of the underlying principals of the daemon could develop further over days, months and even years of highly personal interaction.

(ii) The daemon has agency, but also has strong personal loyalty to its user. This combination is likely to motivate the user who will show empathy with the daemon – naturally showing concern if the daemon is pining and taking delight in restoring it to health and playfulness.

(iii) The daemon can be trained, but in turn it presents important learning opportunities for its user. It can communicate states of fear, threat and uncertainty to the

user in a manner designed to elicit a protective response. Occasionally the daemon may make a mistake (as when a dog bites the postman), but it is important that it can be forgiven for such errors of judgment and taught not to make the same mistakes again. Over time, then, both user and daemon can develop a meaningful and improving understanding of when and where to take risks. We can anticipate that daemons and users who have been together for reasonable lengths of time might both develop sophisticated mental models in relation to security threats and acquire a well-rehearsed and appropriate suite of behaviors for insecure situations.

(iv) The daemon has the capacity to exhibit patience in dealing with an individual – say an older adult - whose static biometrics may be relatively difficult to ascertain. Problems with enrollment or poor quality fingerprints might mean that the imprinting process is a little more time-consuming, but since the daemon accepts reassurance from different sources and comes to know the biometric signatures over time, it offers a much better prospect for inclusivity.

(v) Finally, the daemon has the advantage of longevity – forming a common physical thread through our experience of the world of changing technology. Many of today's devices are designed for a limited life-span (the mobile phone being a good example), but it is important that some systems evoke a sense of persistence. A daemon might be in use for decades – growing old with its owner. Of course a daemon might become lost or stolen, but a stolen (and sickening) daemon would be of no use to anyone. Finally, provided that it is provided with some regular means of recording its stored knowledge of its user, a lost daemon could effectively be reborn (following another trip to the clinic) as a creature with the same loyalties and the same characteristics.

References

1. Adams, A., Sasse, M.A. (1999) Users are not the enemy. Communications of the ACM, 42(12), 40-46.

2. Coventry, L. (2005). Usable Biometrics. In L. Cranor and S. Garfinkel (Eds.) Designing Secure Systems that People Can Use. O'Reilly, pp. 175-198.

3. Cranor, L. and Garfinkel, S. (2005) Preface to L. Cranor and S. Garfinkel (Eds.) Designing Secure Systems that People Can Use. O'Reilly.

4. Cunado, D., Nixon, M.S. and Carter J.N. (2003). Automatic extraction and description of human gait models for recognition purposes. Computer Vision and Image Understanding, 90(1), April 2003, Pages 1-41.

5. Hinde, S. (2004). Banking on security and control? UK companies face overhaul of controls. Computer Fraud and Security, 8, 2-4.

6. Kubala F., Colbath, S., Liu, D., Srivastava, A., Makhoul, J. (2000). Integrated technologies for indexing spoken language, Communications of the ACM, 43:2 (Feb), p.48-56.

7. Little, L., Marsh, S., & Briggs, P. (2006). Trust and privacy permissions for an ambient world. In R. Song, L. Korba, G. Yee (Eds.) Trust in e-services: technologies, practices and challenges. USA: Ideas Group, Chapter 11

8. Livia C. F. Araujo, Luiz H. R. Sucupira Jr., Miguel G. Lizarraga, Lee L. Ling, Joao B. T. Yabu-uti (2004). User Authentication through Typing Biometrics Features. Proceedings of the First International Conference on Biometric Authentication, ICBA 2004, Springer-Verlag Heidelberg, International Conference on Biometric Authentication, 694-700.

9. Mantyjarvi, J. Lindholm, M. Vildjiounaite, E. Makela, S.-M. Ailisto, H.A. (2005). Identifying users of portable devices from gait pattern with accelerometers. Proceedings. (ICASSP '05). IEEE International Conference on Acoustics, Speech, and Signal Processing, Volume: 2, pp. 973-976.

10. Markowitz, J. A. (2000). Voice biometrics. Communications of the ACM 43:9 (Sep), 66-73.

11. Modi, S.K. and Elliott, S.J. (2006). Impact of Image Quality on Performance: Comparison of Young and Elderly Fingerprints. Proceedings of the 6th International Conference on Recent Advances in Soft Computing (RASC 2006), K. Sirlantzis (Ed.), pp. 449-45

12. Montrose, F. and A. Rubin (1997). Authentication via keystroke dynamics. In: Proceedings of the 4th ACM con- ference on Computer and communications security, Zurich, Switzerland.

13. Pullman, P. (1995) Northern Lights. Scholastic.

14. Renaud, K. V. (2005). Evaluating Authentication Mechanisms. in Security and Usability. In L. Cranor and S. Garfinkel (Eds.) Designing Secure Systems that People Can Use. O'Reilly, pp. 103-128.

15. UK families put on Fraud Alert. BBC news, http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm

16. Yan, J., Blackwell, A., Anderson, R. and Grant, A. (2005). The memorability and security of passwords. in Security and Usability. In L. Cranor and S. Garfinkel (Eds.) Designing Secure Systems that People Can Use. O'Reilly, pp. 129-142.