The Biometric Daemon: A Public Perspective

Abstract
Information privacy is maintained through authentication—the act of proving to a system that you are who you say you are. Unfortunately, current authentication methods are affected by a range of usability problems that impact significantly on the security of people’s data and access to secure systems. Recently, an experience-oriented security device, the Biometric Daemon, has been proposed which allows users to authenticate without the need to remember secrets. The Daemon aims to provide easy, natural, and continuous authentication in order to promote more secure practices, but the concept has not, until now, been subjected to critical user evaluation. This paper describes a series of focus groups conducted with the aim of eliciting attitudes and privacy concerns towards the concept of the Biometric Daemon.

Keywords
Authentication, security, transparent authentication, continuous authentication, biometrics, passwords, usability.

ACM Classification Keywords
Introduction
In this paper we consider the Biometric Daemon, an authentication device design recently proposed by Briggs and Olivier [1]. The device has attracted significant interest and is technically feasible, although it remains, at present, a conceptual blueprint. We organised a series of focus groups in order to generate ideas of how users could potentially interact with such a device and to investigate whether the Daemon would be perceived as a secure and usable means of authentication.

The Biometric Daemon
Briggs and Olivier proposed a theoretical device capable of carrying out continuous transparent authentication [1]. The Biometric Daemon would serve to authenticate users in different situations, from websites on the Internet to Automated Teller Machines (ATMs) on the high street. The anticipated uses for the Biometric Daemon are two-fold: as a continuous and transparent authentication device working across multiple platforms, as well as a device serving to alert the user about high-risk transactions [1].

The Daemon’s health and successful operation is primarily dependent upon incidental nurturing that occurs on a daily basis, although deliberate nurturing may provide additional reassurance at key times. Failure to nurture will result in the Daemon ultimately becoming non-active. This may occur if the Daemon is removed from its owner for any significant period. The Daemon is also responsive to its general environment and may need additional assurance when in an unfamiliar setting or asked to execute an unfamiliar transaction (e.g. authenticate at an ATM in an unusual setting). In this way, the Daemon acts as a trust agent—signaling a high-risk transaction to its owner.

Public Opinion
In order to find out what the general population thought about the concept of the Biometric Daemon, four focus groups were organised to investigate user attitudes and concerns. The groups were divided by gender and by age (18-29 years, 30 and over years for both females and males) with four participants in each group. The average age for participants was 32 years.

Perceived advantages
Participants recognised the unacceptable memory load created by password systems—acknowledging that they often had to memorise passwords for several systems, and frequently re-used passwords to offset this problem. Other participants added that they had to change some of those passwords on a monthly basis and that impacted the memorability of the passwords even further.

Participants acknowledged that the Biometric Daemon would alleviate the cognitive problems associated with passwords and PINs as the user would not have to
remember anything. The Biometric Daemon would in effect work as a keychain system—a system that keeps all other passwords in one place.

Participants were also concerned about losing token-based authentication devices or having them stolen. The Biometric Daemon offered them some reassurance on this issue, in that the Daemon’s health would quickly deteriorate if it was apart from its owner and therefore anyone who found it would not be able to access any information with the device.

In regard to biometric systems, participants’ biggest fear was that they would be locked out if something happened to one of their biometric attributes (e.g. cut thumb). Once again, participants found the Daemon reassuring as its reliance on composite authentication meant that a user would be able to cut their finger and still nurture their Daemon with different attributes. For example, the user might use another finger or they might choose to speak to their Daemon.

Perceived disadvantages
A large number of participants worried that they may need to nurture their Daemon frequently and that it would become an inconvenience. In reality most of the nurturing could be done incidentally—although this wasn’t immediately obvious to participants. Clearly the extent to which authentication of the Daemon relies upon implicit or explicit nurturing processes is an issue for further investigation.

Another common security concern was that the Daemon—as an authentication device acting across multiple systems—would become a target for thieves. Participants were reassured that the Daemon would “die” if parted from its owner and all of the information in the device would become inaccessible. Therefore, a thief might be able to obtain a Daemon, but they would not be able to use it to access any services. However a means to then replace the Daemon became a related concern and once again, one for further investigation.

Interaction
Participants were given a small stone and asked to demonstrate how they would deliberately nurture their Daemon if it was in need of some additional reassurance. While the most popular nurturing method was stroking, a large number of participants mentioned that they could envisage themselves using the Daemon to keep their hands busy in order to fulfil their ‘fidgeting’ needs. This suggests that the Daemon could fit into people’s current lives without too much disruption.

Conclusion
The reaction from our focus groups was generally positive, with the device offering a solution to the majority of their concerns regarding current authentication methods. The focus groups helped us understand how the public might interact with the Daemon and raised some issues with the device, although the majority of these were either addressable or desirable.

References