Usability and Acceptability of Biometric Security Systems

Andrew S. Patrick
Information Security Group, Institute for Information Technology
National Research Council (NRC)
286F, M50, 1200 Montreal Rd., Ottawa, ON, Canada K1A 0R6

Andrew.Patrick@nrc-cnrc.gc.ca

Biometric security systems are receiving a lot of attention because of the potential to increase the accuracy and reliability of identification and authentication functions, especially in border-crossing and military applications. A lot of research has been done to assess the performance of biometric systems, with an emphasis on false acceptances and rejections. Much less research has been done on the usability and acceptability of biometric security systems when used by IT professionals and the general public.

A number of factors are increasing the usability of biometric devices. The sensors are getting smaller, cheaper, more reliable, and designed with better ergonomic characteristics. Biometric readers are also being integrated into consumer products, such as mice, keyboards, and cell phones. The biometric algorithms are also getting better, and many systems include features to train the users and provide feedback during use. In addition, biometric devices are being integrated into associated security systems, such as access control and encryption services, to provide a seamless environment.

There are still a number of usability concerns, however. The accuracy of many biometric systems is still not high enough for some applications (i.e., negative identification or matching against a very large database). Also, there is often a negative relationship between the accuracy of a biometric system and the convenience for use, with the most accurate systems (e.g., DNA, Iris, Retina) being the most awkward to use. Biometric devices also have continuing problems handling users with special physical characteristics, such as faded fingerprints, leading to high "failure to enroll" rates. In a field trial of radio frequency fingerprint readers at ATM bank machines, for example, Coventry [2] found a 13% failure-to-enroll rate, mainly due to poor fingerprint images from elderly women.

The design of usable biometric systems is often challenging. Fingerprint readers, for example, can be problematic if the fingers are placed off-centre, moved during the reading operation, or just the tip is presented. Coventry [2] reported that failure to place the fingerprint core at the centre of the reader was a common cause of failures to recognize, and users tended to place their fingers too low on the sensors. Better readers tend to have channels or guides to assist in proper finger placement. Iris scanners can also pose usability problems related to the alignment of the eye with the camera lens. Research in our laboratory and field trial results suggest that this alignment can be difficult at times, and crucial to the success of the application. Moreover, it is often impossible to use the iris scanner and receive feedback at the same time.

And it is not just physical usability issues that are of concern. Ensuring that users understand how to use the entire biometric application is also important. The best systems that we examined incorporated training and feedback so that users could learn the proper use of the biometric technology. Coventry [2] found that providing assistance and direct training during enrollment can greatly improve the acceptance and

performance of biometric systems, but such training can be quite costly.

Concerning the acceptance of biometric security systems, factors that are making the systems more acceptable include technical interest, concerns about identity theft, government border-control initiatives, securing critical infrastructures, and the opportunity to reduce memory demands by replacing memorized passwords. Research has shown, however, that although acceptance is increasing, users are still wary because the benefits are not always evident (both in terms of security and convenience). Angela Sasse [3, 4] has characterized security systems, including biometrics, as “enabling tasks” that differ from the “production tasks” (actual work) that users are interested in. If the enabling task is at all awkward, slow, or unusable, it is natural for users to try to avoid it. For biometrics, perceived convenience can be a bigger driver than any increase in security.

Research studies have found that users’ concerns about biometric misuse and privacy invasions are large and poorly articulated. Potential users are also concerned about the reliability of new technology. Moreover, Coventry [2] found that users report significant fears that criminals may do them harm to obtain the biometric (e.g., cut off their finger). Including "vitality tests" that ensure the biometric is offered by a living person will be crucial to avoid these problems. Observations in our lab suggest that even basic understanding, such as the difference between iris and retinal scans, can be lacking even in sophisticated populations.

There also appears to be a general lack of understanding of biometric templates. Users do not understand, and the interfaces don’t explain, how templates are created, stored, and secured. Our observations suggest that users assume that a complete image of the biometric characteristic is saved, and this leads to heightened concerns about misuse and data aggregation. Since it is obvious to users that the biometric characteristic is not a secret, the applications must explain how the corresponding template is to be kept as a secret, and this explanation is rarely done. Managing privacy impacts and ensuring personal control of biometric use will be very important for promoting acceptance.

Nevertheless, recent studies suggest that people are coming to accept and expect biometric systems. A recent survey of Canadian citizens, for example, found that 80% of the respondents think that biometric systems will be commonly used in the next 10 years [1]. Another study of UK citizens found general support for entitlement cards that include the use of biometrics [5], but that issue continues to be very controversial.

References

[1] Citizenship & Immigration Canada (2003). Tracking public perceptions of biometrics. http://www.cic.gc.ca/english/press/03/poll-biometrics-e.pdf (accessed Oct. 24, 2003)

[2] Coventry, L. (2004). Fingerprint authentication: The user experience. Paper presented at the DIMACS Workshop on Usable Privacy and Security Software, July 7 - 8, Rutgers University, Piscataway, NJ. (http://dimacs.rutgers.edu/Workshops/Tools/program.html)

[3] Sasse, M.A. (2004). Usable security: Beyond the interface. Paper presented at the DIMACS Workshop on Usable Privacy and Security Software, July 7 - 8, Rutgers University, Piscataway, NJ. (http://dimacs.rutgers.edu/Workshops/Tools/program.html)

[4] Sasse, M.A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link': A human/computer interaction approach to usable and effective security. BT Technology Journal, 19, 122-131.

[5] Wearden, G. (2003). Survey gives thumbs-up to ID cards. http://news.zdnet.co.uk/story/0,,t269-s2129590,00.html (accessed May 9, 2003).