When people find security systems difficult or unacceptable, it can result in bottlenecks, excessive operation costs, and shortcuts or workarounds that undermine security. Since 2001, airports worldwide have deployed an increasing number of security systems with biometric recognition. Some operate behind the scenes, for airport staff or cabin crew use. At London City Airport, for example, staff has used biometrics to access secure areas since 2002. At Sydney airport, a face-recognition system called SmartGate (see www.customs.gov.au/site/page.cfm?c=3920) replaced passport checks for Quantas crew in 2003.

Airports have been deploying biometrics for travelers, too. Some systems are voluntary, whereas others are required, and store travelers’ biometric characteristics for inspection or record. The Privium system at Schiphol Airport in Amsterdam and Project IRIS at London’s Heathrow Airport (iris recognition immigration system) are examples of voluntary schemes in which frequent travelers can enroll. IRIS, which uses a two-eye iris-recognition system, stores data about enrolled travelers in a database for identification. Privium uses a one-eye system, and stores a traveler’s biometric details on a card for verification. USVisit and the United Arab Emirates (UAE) Expellee Tracking System\(^1\) are both compulsory schemes. Under USVisit, all visitors holding non-immigrant visas (with limited exemptions, such as for diplomatic passport holders) must provide fingerprints and a digital photograph when entering the US. The UAE requires that all visitors have their iris scanned on arrival, and these scans are checked against a database of people barred from entering.

Airport operators and airlines are adding biometrics to boarding passes or frequent-flier cards to improve security or streamline the traveling process. Most countries are starting to include biometric data (usually digital photographs and fingerprints) in passports and identity cards. It’s likely that, soon, every traveler will encounter biometric systems at every stage of travel. If this happens, such systems must not only support their stated security aims, but travelers must be able to interact with them and find the user experience acceptable. Here, I examine user interaction with such systems, rather than focusing on technical and security issues—readers interested in those aspects can find an excellent summary elsewhere.\(^2\) I also emphasize usability’s importance in successfully operating biometric systems.

**Defining “usable” biometric systems**

Biometric systems should have user-friendly, intuitive interfaces that guide users in presenting necessary traits. Thus, we must ask whether current biometric systems in airports are usable. Are travelers’ user experiences acceptable? To answer these questions, we must first define what “usable” and “user experience” means.

**Usability**

We can assess usability in terms of three criteria: task performance, user satisfaction, and user cost.\(^3\) Systems that the general public uses must also provide universal access. For task performance, we consider an interaction’s effectiveness and efficiency. An interaction is effective if users can achieve their goal and complete the task successfully, and it’s efficient if they can complete it within an acceptable time period. For airport biometric systems, we can focus on two tasks’ performance: enrollment (in which the system captures a biometric and ties it to a
person’s identity), and presentation of the biometric for

- verification (the biometric is checked against a travel record in the database);
- identification (the biometric presented must match a record in a database); or
- screening (the biometric presented must not match those in a database or on a watchlist).

In addition to performance in these areas, we must consider users’ subjective satisfaction with the interaction. Users are unhappy with interactions that impose a high physical or mental workload, or require them to perform actions they find distasteful.

User cost considers the interaction’s impact on users’ health and safety. The system shouldn’t negatively affect users’ physical and mental well-being, either immediately or with longer-term use.

Finally, universal access means that the system must allow anyone who wants to travel to do so—that is, airports must not deny those who can’t provide a certain biometric characteristic the opportunity to travel. Such systems must thus accommodate travelers of different ages and sizes; ethnic, educational, and linguistic backgrounds; and those who have difficulty with certain physical or mental operations.

User experience
All usability criteria might contribute to user experience, but we must consider additional factors. Generally, humans are disappointed when their expectations go unmet. Thus, not meeting user expectations (for instance, in terms of performance) can result in a negative user experience; being denied access or marked as “rejected” is also a negative experience. A product or service’s price, branding, and marketing shape the expectations a user brings to it. The impact a system has on people’s life and work also influences user experience. When UK passports required a digital photograph suitable for face recognition technology, the passport service returned 10,000 of the first 80,000 applications because the photographs didn’t meet all the requirements (see http://news.bbc.co.uk/1/hi/uk/4594674.stm). Rejected applicants had a bad experience due to the extra effort required to send new photos and to possibly thwarted travel plans. A positive user experience is usually based on convenience (time savings or a reduction in physical or mental work), confidence that the system is functioning correctly, and its perceived utility.

Biometric system studies
No formal studies have been done on the usability or user experience of current airport biometric systems in situ. Two large-scale studies of equipment similar to that used in operational schemes have investigated usability and user acceptance. The UK Passport Service Enrollment Trial enrolled nearly 9,000 travelers to test the processes and record user experience and attitude. More than 10 percent of able-bodied and nearly 40 percent of disabled users couldn’t enroll on the iris system tested (which captured both eyes simultaneously). When attempting a one-off verification a week after enrollment, more than 10 percent of able-bodied and disabled users were unable to verify their fingerprint, and more than 30 percent of able-bodied and 50 percent of disabled users failed to verify their facial biometric. Verification times ranged from 39 seconds for the best-performing system to more than a minute for the worst. Even though the UK Home Office pointed out that this wasn’t a performance trial, the results cause concern regarding effectiveness, efficiency, and universal access. In addition to the difficulties disabled users experienced, both the face- and iris-recognition systems had higher failure rates for participants with dark skin and eyes. (With face recognition systems, very dark skin absorbs light to a degree that a face’s underlying topology doesn’t stand out enough; likewise, iris patterns in those with dark eyes didn’t stand out sufficiently.)

The BioPII study enrolled 2,000 volunteer airport staff and asked them to verify for two fingerprint systems, and one face- and one iris-recognition system twice a day, over two months. Not all participants used the system that frequently, and the results showed highly significant differences in error rates and verification times between participants who used the system daily and those who didn’t. The trial included observations and analysis of user interactions, and the report identified “an urgent need to improve the user interfaces and user guidance of all systems tested.” This confirms a previous observation that, to date, usable biometric systems exist in theory, rather than in practice. Although highly practiced users—such as airport staff using systems daily—can overcome some usability problems, few travelers are likely to get sufficient practice.
A personal experience

For smooth operation and positive user experience, biometric systems must be integrated into the real-world process that they’re supposed to safeguard. Consider my user experience with the IRIS system at London Heathrow. Travelers are most likely to notice the system while queuing on arrival for immigration. As you stand there with nothing to do, you notice the occasional traveler breeze past in a separate lane, enter a glass box, and breeze out again. This suggests the possibility of improved efficiency and convenience. But to join the scheme, you must wait for your next trip: enrollment occurs in the departure lounge only, so you have to first plan and add sufficient time to your outbound journey, and then remember to drop by the enrollment office after passing through security.

The enrollment process itself was straightforward:

- First, a passport service official swiped my machine-readable passport through a reader.
- Then, I was directed to a desk, where I sat opposite a staff member with a PC and digital camera; under the camera was a screen facing me. The system captures both eyes, and I could see my face and target lines on the screen.
- Once my eyes had been captured, I was asked to look into the camera again, using the image on screen to guide me.
- Finally, I was handed a printout confirming my enrollment and passport data, and staff explained that I would have to walk up to the booth, look into a camera again, and wait for verification (a process that should, according to the UK Home Office Web site, take 20 seconds.) I received a paper slip confirming my enrollment and passport details and an “Arrival Guide” leaflet (see Figure 1) that explains how to use the system.

![Figure 1. Arrival Guide leaflet. This leaflet describes how to use the UK’s IRIS system at London Heathrow Airport.](image)

The whole process took 7 minutes (there was no waiting time when I enrolled) and was free. My husband also enrolled successfully, with his glasses on.
Arriving back at Heathrow three weeks later on a red-eye, I headed for the IRIS booth, passing queues of other travelers. I faced a different interface from the one I had enrolled on: rather than sitting down and having the camera adjusted to me, I stood in front of three windows that, on closer inspection, turned out to be cameras. Depending on your height, the system determines which of the three cameras you should look into. Unless you’re exactly the right height for the camera, you have to bend forward to bring your face into the camera’s field of view. Once you see your face in the camera, you have to first move your face sideways to position one of your eyes in the target circles shown, and then move your whole body backward or forward to be at the correct distance. The resulting “bendy shuffle” can take some time. The system provides voice feedback, but it’s general (“move forward/backward”) and slow to arrive. Rather than assisting users in presenting their biometric feature, the system requires them to put their bodies in the right position. This is, unfortunately, typical for current camera-based systems for face and iris recognition. Systems with automatic height adjustment and autofocus are available and result in significantly better performance. The iris recognition algorithm’s inventor, John Daugman, told me that deployments that do use them, such as the UAE system, don’t have these problems. However, Lynne Coventry from NCR UK, mentioned that many purchasers aren’t keen on adding these features because they increase equipment cost and size. This seems shortsighted: I use the IRIS system roughly once a month, and end up doing the “bendy shuffle” every time. I’m not the only one, and as more people have enrolled in the IRIS scheme, the booth now has queues at busy times.

Accepting a system

What about user acceptance? In the BioPII trial, most participants rated the interaction with the four systems they tried either satisfactory or positive. But in the post-trial questionnaires and focus groups, they raised several usability and acceptance issues. With the iris system, questions about safety were most frequent—many members of the general public confuse the unfortunately labelled “iris scan,” which takes a photo, with a retina scan, which casts a beam of low-energy infrared light into a person’s eye to scan the pattern of blood vessels at the back. For fingerprint systems, hygiene is the primary concern. My own experience of several enrollments in the USVisit system is that the fingerprint sensors usually look dirty (fingerprints largely consist of fatty skin secretions called lipids). It might not affect the performance of the high-end optical sensors, and in terms of hygiene, touching a fingerprint sensor is no different from touching a door handle. But the illuminated sensor shows visible dirt, so many travelers’ instinctive response is, “yuck.”

I haven’t used the Privium system at Schiphol Airport myself, but I have interviewed a number of travelers who have. It’s a one-eye iris system in which users can adjust the height, so they don’t have to bend down (see Figure 2). Some users had difficulty positioning their eye in the relatively small target area, especially after “arriving on the red-eye, when I can’t open my eyes properly and blink all the time.” An interesting difference between Privium and Project IRIS is that Schipol Airport authority charges travelers to enroll. Then, they receive a card that stores their iris template. A Web site gives detailed information about the system, including answers to frequently asked questions that many users have about health and safety, data protection, and so on. In addition to the basic service (which has provided automated border control since 2002), the authorities now offer a premium-rate service with additional benefits, such as valet parking. Travelers respond positively to the service because it offers convenience and makes them feel “privileged.”
We can learn several lessons from these experiences about deploying biometric systems in airports. First, choose a system that makes correct presentation of the biometric easy. A cheaper system that makes presentation difficult will reduce performance and lead to negative user experiences. You should also design all the processes the traveler encounters to be as easy and pleasant as possible. Enroll travelers on the same setup they’ll be using for verification. Usability—check the entire setup (for instance, access to the booth). Provide step-by-step guidance and feedback. Make sure the system is clean and pleasant to use.

You should also budget for testing and improvement phases—you’re unlikely to get a smoothly operating system out of the box. Finally, think about benefits for travelers, not just about security. The travelers’ goal is to get from A to B—safely and securely, yes, but if security makes getting from A to B too hard, it can be counterproductive. Making the security part of a system that offers convenience to travelers, as in the Schiphol example, is the way to ensure positive user experiences.

References


**M. Angela Sasse** is the Professor of Human-Centred Technology at University College London. Her research interests include usability and effectiveness of security systems. Sasse has a PhD in computer science from the University of Birmingham, UK. She is a member of the ACM and the British Computer Society. Contact her at a dot sasse at cs dot ucl dot ac dot uk.

**Editor: S.W. Smith, sws at cs dot dartmouth dot edu**

**Related Links**

Purchase or Digital Library members log in:

- May/June 2007 Digital Library issue (You must have a subscription to access the articles)

**Cite this article:**