The Science Behind Passfaces

June 2004

The Science Behind Passfaces

Theory and Practice

This document is divided into two main sections: ***Section One*** *–* ***"Theory"*** *– summarizes the scientific research on the physiology and advanced cognitive psychology behind the Passface™ system and* ***Section Two*** *–* ***"Practice"*** *– describes some of the design considerations in its implementation. It is intended for the general reader: the references include links to more detailed notes, scientific papers, their authors and institutions.*

Section One - Theory

Most people find it very hard to remember passwords and PINs yet the human brain is amazingly effective at the apparently harder task of remembering and *recognizing* individual faces. The Passface™ system exploits this ability to provide a robust and intuitive authentication mechanism.

The underlying principle of the Passface™ system is supported by extensive academic input and experiment. The experiments were conducted by Professor Hadyn Ellis [1], Head of the School of Psychology at University of Wales Cardiff and a world authority on face recognition. The extensive research behind these experiments goes back to the 1970s when efforts on machine recognition of faces began in earnest and researchers started trying to emulate the human brain. The Passface™ system does not try to emulate the brain, it actually uses it.

The research [2] is concerned with trying to discover how the human visual brain works and specifically how it perceives, remembers and recognizes faces. This in turn is linked to research on how the whole brain works; from down at the cell level right up to research on what is "consciousness". As well as many direct experiments on cognition there is also significant data obtained from the study of people whose brains have been affected by injury or illness and who exhibit very unusual cognitive behavior e.g. an inability to recognize the faces of even members of their own family - a condition known as prosopagnosia.

How the human brain works is still largely a fascinating mystery and science in this area is still in its first steps. It is now largely accepted the brain is not just a big computer, it has many unique processes that are not understood as yet, let alone how these processes function in neurological terms. The brain appears to have evolved special components to handle special tasks that may have been crucial to our survival. There are even separate processes involved in learning a new face and subsequently recognizing it. At the cell level for instance we have different neurons for seeing horizontal lines and sloping lines.

The Science Behind Passfaces

How we perceive faces

It has now been demonstrated both by inference and direct neurological measurement that we have in our brains a special component whose sole function is to recognize faces. The speed of operation and reliability of this component is significant in making the Passface system so intuitive and natural and therefore effective. Viewing and recognizing faces is not just the same as looking at other objects - it is special:

- A human infant is born with a capacity to recognize faces and shows a preference for looking at faces well within the first hour after birth;
- An infant can recognize its mother after only 2 days;
- We know that we have seen a familiar face before after only twenty thousandths of a second (20ms);
- In one experiment people recognize schoolmates they had not seen for 35 years with over 90% accuracy.

The brain has a short-term "iconic" memory (like a computer's cache) which holds the image before it is transferred to long-term memory. The iconic memory is overwritten by a new image, so we need to see something for a finite time (about 1 second) if we are to remember it. Which part of the brain is being used for different functions can be measured by monitoring blood flow with a PET scanner. When a part of the brain is active its blood flow increases. The part of the brain primarily concerned with face recognition is in the right parietal lobe (right side upper middle) but other parts are also involved. Generally the right side of the brain is concerned with pictures and spatial relationships, the left more to do with abstract processes like mathematics and also language. Passwords use left brain; the Passface™ system uses the right brain. As the saying goes "a picture is worth a thousand words".

How we remember faces

This is the least known of the face related brain processes: As previously mentioned, it is not just a variation on recognizing a known face.

Some faces are more distinctive than others and the more distinctive the easier it is to remember. People of all genders and races have broad agreement on whether a face is distinctive and whether it is attractive.

The context in which we know the face is also important. There is an anecdote of a man approaching Oscar Wilde and saying, "you must remember me, we met in Birmingham", to which Wilde replied, "no doubt if we were in Birmingham I would remember you again". The anecdote has a basis in truth.

The Science Behind Passfaces

How we recognize faces

In our evolutionary past it has been vital we recognize quickly friend or foe or stranger and evolution has given us a special cognometric[1] process to deal with it. It appears that the brain may store faces in some sort of spatial relationship. The more distinctive a face then the fewer other faces there are like it: it is recognized more quickly because there are more elements that are unique to it and fewer elements common to many others. These elements do not appear to be dimensions and parts of a face but more grades of texture and overall shape. Face recognition is a holistic process; our brains do not analyze faces into portions. It is also unaffected by age (although putting a name to the face may be - fortunately, the Passface™ system does not require this)

Emotion helps: one is more likely to recognize someone with a definite expression than a neutral one. For this reason, caricatures emphasize and exaggerate not only distinctive features but also expressions. We would obviously prefer to look at happy faces than sad or menacing ones. There is general agreement across gender and race of what different expressions mean; it appears to be innate. We also all appear to agree on ascribing personality to different types of face despite the demonstrated fact that there is no correlation between any type of face and personality. Type of face in this context does not include lines of age and experience. It would be difficult to quarrel with Mark Twain's observation that "by the time a man's forty, he's responsible for his own face".

Context is important; someone we met on the beach on holiday we may not recognize in the bar later, with the inevitable cliché: "I didn't recognize you with your clothes on". As adults, we tend to recognize more easily people whom we perceive as important to us.

The quality of the image may be very poor, distorted or of only a small number of pixels; nevertheless we can still recognize someone we already know. Color is unimportant; there are famous portrait paintings (e.g. Van Gogh) where facial features may be colored red or green, but one is not conscious of these unrealistic colors, only the textures and shading.

If you have just seen a face you will recognize it again more quickly than if you had not just seen it: this process is called "repetition priming". Moreover if you have just seen a face that has a relationship to another you will recognize the other more quickly. If you

---

1 Cognometric (kagnωεmετriks) 1. n. a measurable, innate cognitive ability of the human brain (e.g. ability to recognize a familiar face or musical tune). 2. n. method of personal authentication based on measuring an innate cognitive ability of the human brain (e.g. ability to recognize a familiar face) [C21: from Latin accognoscere, to recognize + Greek metro, measure.]

have just seen George Bush you will recognize Laura Bush more quickly. This is known as "semantic priming"

The speed of recognition also depends on how familiar we are with that person's race. The phenomenon called the "other race effect" describes how we appear to recognize someone of our own race quicker than those of another race. However, other research indicates that if we are used to interacting with other race face types we are almost as effective as with our own.

Identifying to whom a face belongs is a further and somewhat different process. It is interesting that there appears to be no tying up between faces and names, so an inability to put a name to a face is a common occurrence. Indeed it has been shown it is easier to put an occupation to a face than a name.

There is no evidence that a person's ability to recognize faces deteriorates with age. Indeed the evidence is that adults are better than young children.

Section Two - Practice

This section describes how these scientific elements have been incorporated into the Passface™ system. Further detail is available: see reference [3].

Note: Passfaces do not require the user to identify a face - only to recognize that it is familiar. This means that the commonest area of concern - "I recognize that person but can't remember their name" - is not an issue.

Configuration

The basic configuration of the Passface system (five passfaces, one to be selected from each of five successive grids of 9 faces) has been chosen by taking into account a combination of security, usability and practicality considerations.

In principle, it is possible to implement the Passface system as any number, N, of P by Q grids, with the user having M passfaces faces per grid (provided M < P x Q / 2) – the formula for the number of permutations being:

$$[(P \times Q)! / M! \times (P \times Q - M)!]^N$$

However, it has been found by experiment that having overlarge grids or more than one passface per grid can be difficult or even confusing for the user. (Also note that the effective entropy of each passface is reduced if there is more than one per grid – this becomes very significant unless M is much smaller than P x Q. For example: the number of permutations of 3 passfaces picked from 3 separate 3 by 3 grids is 729; whereas 3 passfaces picked from the same 3 by 3 grid provides only 84 possibilities!) The 3 x 3

grid has the obvious advantage that it maps directly to a numerical keypad – allowing the Passface system to be used on devices such as ATMs and Web TVs where this may be the only means of user input.

Using five passfaces picked from five 3x3 grids provides 9^5 combinations (i.e. a 1 in 59,049 chance that someone could guess them at random) which is sufficient for most consumer and business applications – provided, of course, that the system is not open to exhaustive search by an attacker. For comparison, consider the four-digit user-selected PIN used globally on ATM networks: the chances of someone guessing a PIN are less than 1 in 10,000 (users traditionally select from a much smaller set of numbers that are memorable such as dates and telephone numbers) yet because an attacker only has only three tries before the system locks him out, this has proved quite adequate as a means of authenticating the card owner. Again, if the application or the security administrator demands higher security, then more than five passfaces can be used; there is no known limit to the number of faces that a person can remember.

Display parameters

The size of the displayed images has been chosen to allow the full grid to be easily perceived (on an average-sized computer monitor) without requiring excessive head or eye movement. Our experience has shown a wide variation in how people look at the grid of faces: some scan from left to right and top to bottom as if they were reading, others follow a zigzag path while some spiral out from the center; some don't seem to scan at all – they seem to take in the whole grid with a single glance

Images are color and shown in a portrait format as this is a very natural way of seeing people. However, showing the faces as grayscale is not detrimental to ease of recognition for the users – the passface system works equally well on a Palm Pilot for example. Highly security-conscious security administrators may even opt for grayscale on all platforms in order to make it even harder for a user to describe their passfaces to someone else.

In some high-security applications the grids of faces may be displayed only for a very short time – around half a second is long enough for practiced users to recognize their passfaces. When this timing is combined with "masking", where all the faces in a grid are overwritten with a common mask face, it becomes extremely difficult for "shoulder surfers" to learn the passfaces as the user clicks on them – even with the collusion of the user. (The mask has the effect of overwriting the shoulder surfer's short-term iconic memory – as referred to previously). Since the legitimate user already has the passfaces in their long-term memory the mask has no effect on them. This mask face can also be used as a primer by displaying it before the challenge.

Face sets

A user's set of (usually five) passfaces is chosen randomly by the system so that all faces in each of the logon grids are equally likely. As well as providing the "constant entropy" that is a feature of the Passface™ system, this also has the benefit of making it easier for the users to enroll with the system since they do not have to worry about which faces to choose. (Note that having system-selected passfaces presents no more of a challenge for the users' memory – it merely reflects our normal experience: we don't get to choose the faces of our associates at work, yet we always recognize them when we see them.) Contrast this with passwords which, if system-selected are difficult to remember and if user-selected present a challenge for the user to come up with something "secure" and memorable. Today most systems employ user-selected passwords. Even when policy rules are imposed on their construction, the distribution is not Uniform, which means that there are always "weak" entries that reduce the overall security of the system.

The grids of faces in the Passface™ system are grouped by sex and, as far as possible, are selected to be equally distinctive so that the passfaces cannot be (partially) described by gender or obvious characteristic. Further, none of the faces has a tendency to stand out from the others. Only when a Passface is shown subsequently at login, will it then seem (to the user who is familiar with it) to stand out from the other eight "decoy" faces in the grid.

The faces used are recorded especially for Real User with a digital movie camera. Subjects are lit primarily from above and to the right, which is a "natural" lighting position and shows the texture and shading of faces. (Note: all subjects are required to sign a model release allowing Real User to use their image.)

Note that, at login, a passface is always seen in a grid with the same eight decoy faces. Clearly, if the decoys varied between login sessions, then it would make it easy for an attacker to identify the passface as the constant. This may at first sight seem to present a problem since the user might be expected to eventually become familiar with the decoy faces and start confusing them with her passfaces. However, our experience and trials have shown that, although the users do indeed gain a certain level of familiarity with the decoys, their speed and accuracy at recognizing their passfaces actually increases. It seems that each login reinforces the user's familiarity with their passfaces more than with their decoy faces.

Enrollment

Cognitive psychologists assure us that people can easily recognize familiar faces. Our job is to assure that the familiarization process is adequate. The Passface™ system enrollment process has been optimized, through trials carried out by Professor Tim Valentine, Head of Department of Psychology at Goldsmiths College, University of

London, so that users spend a minimal amount of time enrolling (3 to 5 minutes is typical) yet will all become sufficiently familiar with their passfaces to recognize them if they see them within one week of enrollment. The trials and subsequent analysis of usage data from the Real User site (where over 8,000 people have enrolled) have demonstrated that, provided users are required to login to the system at least twice in the first two weeks following enrollment, they will be able to reliably login again after more than six months of not using the system.

Enrollment consists of two phases: "introduction" and "practice". During introduction, the Passface™ system is explained and the user is shown (i.e. introduced to) each of her passfaces individually. Practice requires the user to go four times through the process of picking out each of her passfaces in turn from five grids of nine faces – exactly as a normal logon except: during the first time, the passfaces are emphasized by movement so as to draw attention to them and help "imprint" them on the user's brain; and, during both the first and second times, if the user makes a wrong selection (i.e. picks a decoy), this will be indicated by a large red cross appearing on that selection. If the user does select a decoy during any iteration of the practice, she will be required to repeat the process from the previous iteration. Therefore, in order to complete enrollment, the users must get through at least four iterations of practice without picking a decoy; this ensures that by the end, they really are familiar with their passfaces. (By then they are, of course, also familiar with the logon process.)

Bibliography and references

[1] Professor Hadyn Ellis School of Psychology University of Wales Cardiff

[2] The Face Recognition Home Page

[3] The Visage System - a Psychological Evaluation of Parameters - N. Mosdell, H. Ellis, A Quale, University of Wales Cardiff. (Available on request)

[4] In the Eye of the Beholder - Bruce, Vicki - Young, Andrew

~ End of Document ~

