ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

System Security by Measuring and Analyzing Biological Data Authentication Modalities

Divya Rathi*, Anu Rathi, Aditya Kumar
* Department of CSE, JPIET, Meerut, India
Department of CSE, VCE, Meerut, India
divyarathimzn@gmail.com

Abstract

Most biometric verification systems are done based on knowledge base and token based identification these are prone to fraud. Biometric authentication employs unique combinations of measurable physical characteristics-fingerprint, facial features , iris of the eye, voice print and so on- that cannot be readily imitated or forged by others We examine three biometric authentication modalities – voice, face and gesture as well as password entry, on a system, to explore the relative demands on user time, effort, error and task disruption. Our laboratory study provided observations of user actions, strategies, and reactions to the authentication methods. Face and voice biometrics conditions were faster than password entry. Speaking a PIN was the fastest for biometric sample entry, but short-term memory recall was better in the face verification condition. None of the authentication conditions were considered very usable. In conditions that combined two biometric entry methods, the time to acquire the biometric samples was shorter than if acquired separately but they were very unpopular and had high memory task error rates. These quantitative results demonstrate cognitive and motor differences between biometric authentication modalities, and inform policy decisions in selecting authentication methods.

Keywords: Authentication, biometric, usability, gesture.

Introduction

Authentication by biometric verification is becoming increasingly common in corporate and public security systems, consumer electronics and point of sale (POS) applications. In addition to security, the driving force behind biometric verification has been convenience.

Biometric devices, such as finger scanners, consist of:

- A reader or scanning device
- Software that converts the scanned information into digital form and compares match points
- A database that stores the biometric data for comparison

To prevent identity theft, biometric data is usually encrypted when it's gathered. Here's how biometric verification works on the back end: To convert the biometric input, a software application is used to identify specific points of data as match points. The match points in the database are processed using an algorithm that translates that information into a numeric value. The database value is compared with the biometric input the end user has entered into the scanner and authentication is either approved or denied. User frustration with password-based authentication on system demonstrates that a high level of usability must be achieved for a system authentication technique to be accepted. As biometric recognition algorithms continue to improve, the user experience will be an increasingly critical factor in the success of such techniques.

In this paper, we explore authentication techniques on system from the users' point of view. We study three biometric authentication modalities - voice, face and gesture, and combinations of voice with face and gesture. A typical 8-character password condition is included as a baseline. This study is the first to measure user action times for authentication using different biometrics on a system. It provides insight into user performance when using these techniques under favorable conditions.

The study examined:

1. The time taken to provide an authentication sample (password, biometric, or two biometrics);

2. Error rates in providing a sample of suitable quality for analysis by verification algorithms;

3. The impact of the user actions required for authentication on performance in a memory recall task

4. User reactions to the authentication methods.

To allow for comparison between authentication methods, the voice and gesture conditions use the same 8-digit authentication token. We find that speaking was the fastest biometric authentication method, but taking a photograph supported better performance in the memory recall task. Speaker verification was considered less usable than password, face and gesture (writing an 8-digit PIN). Combination conditions – simultaneously entering two biometric samples were very unpopular. Failure rates were not significantly different among single conditions, but combining methods led to high error rates.

Biometric modalities

There are various biometric traits a human being possesses which can be used.

A. Physical modalities: This is related to the shape of the body. This includes fingerprint, iris, hand geometry, face, retina, ear shape, DNA etc. recognition system.

B. Behavioral modalities: These are related to human behavior that may change over time, like signature, typing rhythm etc.

C. Both physical and behavioral: For example voice, as a physical characteristic voice is constant because it depends on the size or shape of the mouth, lips, vocal tracts and nasal cavities etc. But for the behavioral part, voice is not constant. It can be changed based on individual's emotion, sickness or age.

A. Physical modalities

a. Fingerprint recognition: A fingerprint is made up of ridges and furrows. Uniqueness is determined by ridges, fur-rows, the minutiae points. Fingerprint is one of oldest and most popular recognition technique. Every individual pos-sesses unique finger patterns, even twins has different patterns of rings and furrows.

b. Face recognition: Face recognition is based on both the shape and location of the eyes, eyebrows, nose, lips and chin. It is non intrusive method and very popular also. Facial recognition is carried out in two ways [5] [6]:

- **Facial metric:** In this location and shape of facial attributes (e.g. distances between pupils or from nose to lip or chin) are measured.
- **Eigen faces:** Analyzing the overall face image as "a weighted combination of a number of canonical faces."

c. Iris recognition: The iris is the elastic, pigmented, connective tissue that controls the pupil. The iris is formed in early life in a process called morphogenesis. Once fully formed, the texture is stable throughout life. It is the most correct bio-metric recognition system so it is called as king of biometrics. The iris of the eye has a unique pattern, from eye to eye and person to person. Eye color is the color of iris. Iris recognition uses camera technology with subtle infrared illumination to acquire images of the detail-rich, intricate structures of the iris [9].

d. Retina scan: The blood vessels at the back of the eye have a unique pattern, from eye to eye and person to person. A light source is needed because retina is not visible. The infrared energy is absorbed faster by blood vessels in the retina than by the surrounding tissue. Based on this pattern of blood vessels can be easily recognized. It is required that a person remove its glasses, focus on a specific point for about 10-15 seconds. A coupler is used to read the blood vessel patterns. A coherent light source is also required for illumination [10].

B. Behavioral modalities

a. Gait recognition: It means how the person walks. Gait is the pattern of movement of the limbs of animals, including humans, during locomotion over a solid substrate. Patterns include overall velocity, forces, kinetic and potential energy cycles, and changes in the contact with the surface (ground, floor, etc.).Gait recognition also takes into account the gender of the person because there is difference in the way of walking of males and females [14].

b. **Signature**: A signature is a handwritten (and sometimes stylized) depiction of someone's name, nickname that a person writes on documents as a proof of identity. Signatures have been accepted in government, legal, and commercial transactions as a method of authentication.

c. **Keystrokes**: It is the way a person types on keyboard. I include speed, how the buttons are pressed and released. It changes from person to person [16].

C. Both physical and behavioral

a. Voice recognition: It focuses on the vocal features that produce speech and not on the sound or the pronunciation of speech. The vocal properties depend on the dimensions of the vocal tract, mouth, nasal cavities and the other speech processing mechanism of the human body. There are three different techniques [11]:

- **Text-dependent systems:** The user is requested to speak a word or phrase which was earlier during the enroll-ment process. It is matched with stored pattern.
- **Text-prompted systems:** The user is prompted to repeat or read a word or phrase from a pre-recorded vocabulary displayed by the system (e.g., *"Please say the numbers 7 8 3 4!"*).
- **Text-independent systems:** Systems have no initial knowledge /vocabulary. Reference templates are generated for different phonetic sounds of the human voice, rather than samples for certain words.

Usability study

Three different forms of user action for biometric authentication, password entry, and two combinations were examined in six experimental conditions described below. All voice and gesture conditions used the same authentication phrase, '35793579', providing a memorable consistent value across both modalities, and an audio sample long enough to be acceptable for an automated speaker verification technology. A repeated 4-digit sequence was used to increase memorability while still using a variety of gestures and speech sounds. Password entry was included as a reference point. This paper uses the terms 'user action' and 'taking action' to refer to the actions taken by the user in providing an authentication sample (biometric or password). As authentication algorithms improve, these user actions will be an important determinant of technology acceptance. This study assumes a zero false rejection rate (FRR), the ideal scenario for a legitimate user. The six experimental conditions were as follows:

1. Password: Enter an alphanumeric password using the built-in on-screen keyboard. In the spirit of typical corporate password policies, the easy to remember 8-character password *securit3* was used.

2. Voice: The user must speak the password phrase "three five seven nine three five seven nine".

3. Face: The user must take a photograph of their face using the front-facing camera.

4. Gesture: The user must write '35793579' on the screen with their finger.

5. Face+Voice: The user must say "three five seven nine three five seven nine" while simultaneously lining up their face and taking a photograph.

6. Gesture+Voice: The user must say "three five seven nine three five seven nine"while simultaneously writing the digits '35793579' on the screen with their finger.

A. Candidates

Participants were 30 employees (13 women) of a large technology corporation, unconnected to the project, having 1.5 to 45 years with the company. They were recruited through email lists and personal contacts, and were given a small compensation. Twenty-nine have experience using a smart phone. Six use multiple smart phones. Twenty-one have used a tablet device with the iPad being the most common device and one month to two years of experience. Five used a smart phone and three used a tablet device to access protected company information, where policy required a mobile device screen lock password of at least 8 characters, including both alphabetic and numeric or symbol characters. All participants had experience with password and PIN as an authentication method. Five occasionally used on-screen signature, four regularly used other types of gesture id and one occasionally did. Six occasionally used face id (3) or voice id (3). Ten occasionally used fingerprint while one regularly did. Some participants' work had at some time involved taking or analyzing facial images for verification (4), recording or analyzing speech samples for voice or speaker verification (7), or collecting or analyzing gestures (3).

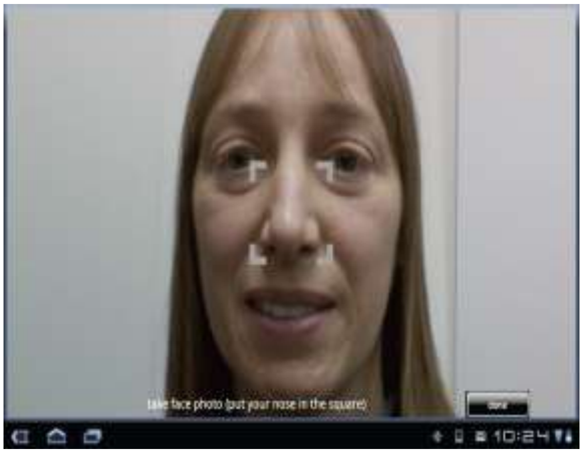


Figure 1: Face Authentication Screen

B. Procedure

After providing informed consent, participants used six different forms of authentication action, presented in random order, and then filled in the demographic questionnaire. We chose to use a standing position. This makes interaction more challenging because the user must hold the device while operating it, and enabled participants to explore different lighting positions easily. All were advised that they could lean on a desk or a wall, move freely around the room as they wished, and rest at any time. For each condition, a researcher showed a printed image of the authentication screen and described the user action to be taken. On-screen instructions were also provided. The instructions for taking a photograph were "Authenticate by taking a well-lit photo of your face. Put your nose in the box and use a neutral expression. Press 'done' when you are ready to take the photo." When Face was combined with Voice, participants were instructed to "Authenticate by saying the PIN AND taking a well-lit photo of your face. You can speak while lining up your face, or speak first and then take the photo. Put your nose in the box and use a neutral expression. Press 'done' when you are finished speaking AND are ready to take the photo." In the Gesture + Voice condition, the instructions were: "Authenticate by saying the PIN AND writing it on the screen with your finger. You can write and speak at the same time, or in any order you choose. Press 'done' when you have finished both writing and speaking". Participants executed 3 practice trials then went on to a set of 8 memory task trials. They were not told that the system was not performing automated verification of their face/voice or gesture. A researcher observed participant actions, comments, position, and method of holding the tablet device. In voice conditions, participants were corrected by the researcher if they did not say the correct phrase. It was not possible to see their gestures during the sessions. After completing each condition, participants sat down to fill in the usability questionnaire. This provided an opportunity to rest. The instruction given for the usability evaluation questionnaire was:

"Where these questions ask about "the method" we mean the authentication method you just used, within the context of the scenarios where you are trying to remember a number and unit. This includes the experience of sometimes having to repeat your actions to get a good sample, or correct an error. For example, 'learning to use the method' means learning how to use it accurately, to avoid the need to repeat."

C. Data Available

Two participants ran out of time and attempted only 5 of the 6 conditions. A further 16 trials are missing due to technical problems. Three participants did not complete all conditions because they were unable to provide either face or voice samples that passed the acceptance test (see below for further details). Finally, one participant abandoned the Gesture +Voice condition after 2 scenarios due to frustration with that method.

Data from one participant, whose comments indicated that he was testing the authentication mechanisms rather than performing the requested tasks, were discarded.

Authentication attempts were coded as follows:

1. Success: The participant performed authentication correctly and was successful. (1229 samples)
2. Minor error: The participant performed well enough to succeed but may have included additional speech or corrected errors. (43 samples)
3. Error: The user attempted to provide the correct authentication but failed, for example a password with errors, a fuzzy picture, or a speech sample that did not meet the quality check. (100 samples)
4. Noncompliance: The user did not perform authentication correctly, for example speaking the value to be memorized ('529mg') instead of the PIN, saying nothing, or writing a squiggle. (35 samples)
5. Technical error: The sample was unusable due to technical problems. (14 samples, all empty or clipped speech files) Technical errors and noncompliant attempts were excluded from the analysis.

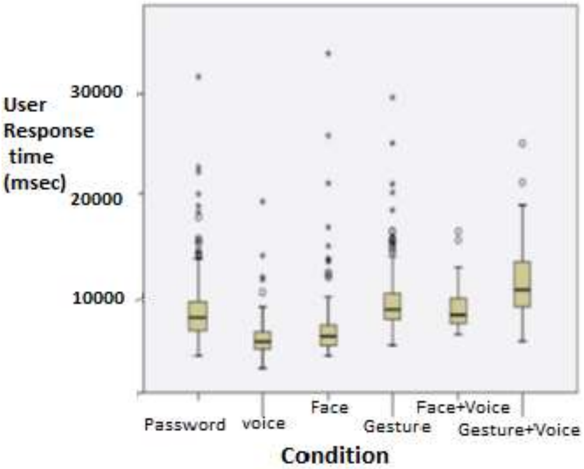


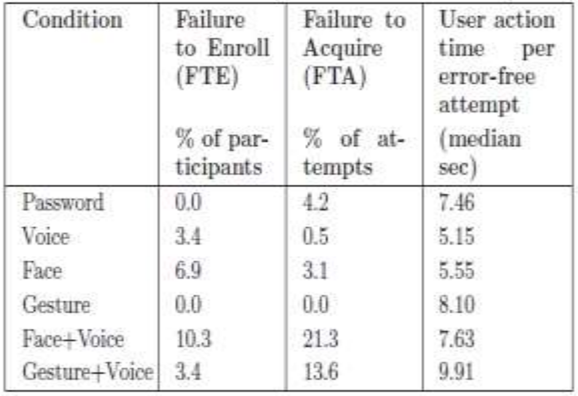
Figure 2: User response time by authentication condition

Results

A. Failure to Enroll

The 'Failure to Enroll' metric (FTE) used in biometric usability research [10] is intended to identify the proportion of individuals who would never be able to use a biometric system. Table 1 summarizes the failure to enroll (FTE) rates for each condition. Two of the 29 participants found that the Face condition did not work for them – they were not able to take a picture in which the face verification engine could locate their face.

Table 1: Biometric performance summary



Condition	Failure to Enroll (FTE) % of participants	Failure to Acquire (FTA) % of attempts	User action time per error-free attempt (median sec)
Password	0.0	4.2	7.46
Voice	3.4	0.5	5.15
Face	6.9	3.1	5.55
Gesture	0.0	0.0	8.10
Face+Voice	10.3	21.3	7.63
Gesture+Voice	3.4	13.6	9.91

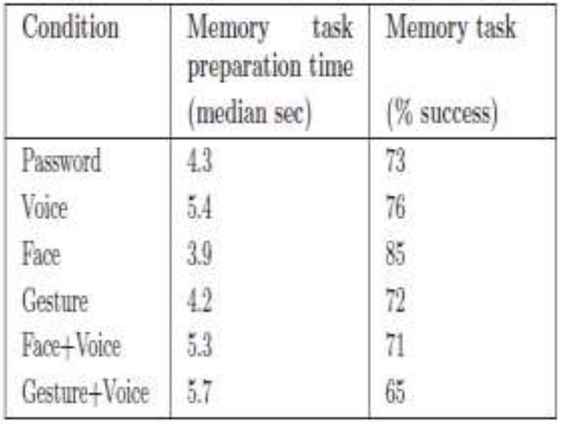
B. Failure to Acquire

The 'Failure to Acquire' (FTA) metric [10] is used in biometric usability research to measure failure to provide a sample of sufficient quality. In this study it captures failures where a participant provides a sample that does not meet the predefined quality criteria. For biometric samples, such samples do not contain good enough data on which verification algorithms can operate. 1372 user actions were analyzed, of which 92.7% were successful. Table 1 summarizes the percentage of these attempts that were unsuccessful, in each condition.

C. Memory Task

The memory task required participants to enter a three digit value and two-digit measurement unit they had been shown prior to the authentication action, using the on-screen keyboard. Trials containing technical errors or noncompliant attempts are excluded (N=21), leaving 1277 trials for analysis. Table 2 shows the median memory task preparation time, defined as the time participants spent viewing the screen that showed the value before proceeding to the authentication screen. This gives an indication of time spent actively memorizing the value.

Table 2: Memory task performance summary



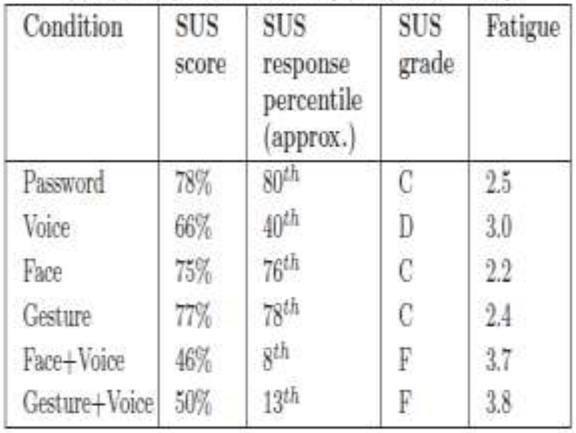
Condition	Memory task preparation time (median sec)	Memory task (% success)
Password	4.3	73
Voice	5.4	76
Face	3.9	85
Gesture	4.2	72
Face+Voice	5.3	71
Gesture+Voice	5.7	65

D. Responses

Table 3 summarizes the overall score, percentile and grade for the System Usability Scale (SUS) for each condition, and level of agreement with the question “This method was tiring to use”. These interpretations illustrate that none of the user actions were well liked in the context of the memory task, with grades ranging from C to F. Password, Face and

Gesture were rated above the average SUS response value, while the combination conditions lagged behind, with ratings in the 10th percentile of typical responses. The combination conditions were also considered the most tiring to use, while Password, Face and Gesture were not tiring.

Table 3: System Usability Scale summary



Condition	SUS score	SUS response percentile (approx.)	SUS grade	Fatigue
Password	78%	80th	C	2.5
Voice	66%	40th	D	3.0
Face	75%	76th	C	2.2
Gesture	77%	78th	C	2.4
Face+Voice	46%	8th	F	3.7
Gesture+Voice	50%	13th	F	3.8

Discussion

These data provide an understanding of the relative user effort required by the different authentication mechanisms under quiet, well-lit, stable conditions and may be representative of environments such as an office or home location. Work is ongoing on robust authentication algorithms that are effective in a broad range of environments that are noisy, low lighting, or involve movement (e.g., walking, public and private transportation), etc. and multi-factor biometric authentication. Privacy considerations may be addressed by cancellable biometrics [26].

The interfaces for biometric and password acquisition used here were simple. With the exception of a screen orientation to facilitate self portrait photos (landscape), we did not attempt to compensate for any perceived shortcomings of the device (e.g., reflections on the display surface, alternative keyboard layouts to minimize changing between alphabetic and numeric/symbol layouts). Our participants were novice users, and performance improvements with practice could be expected. Further field studies in natural environments with more experienced users are needed to provide a more complete understanding, including learning effects.

A. Time to provide an authentication sample

Clearly the Face and Voice conditions were faster than the Password and Gesture conditions. The Gesture entry was significantly slower than any of the other conditions, although that may be related to the substantial software lag time in responding to drawing on the touch screen. On average, the Face and Voice conditions had a 2.0-2.5 sec. lower user action time than the 7.5 sec. in the password condition. Participants were able to provide dual biometrics in less time than sequential entry of the same two biometrics, but with higher acquisition error rates. The error free Face+Voice condition time was comparable to error- free password typing. Where there is a failure to provide an acceptable biometric sample, the overall time would quickly rise, underscoring the importance of an authentication interface that minimizes user error through appropriate feedback to the user, and recognition algorithms that can operate on real-world samples with minimal error. For the Face conditions, once participants found a place with good lighting, they tended to stay in that position. In outdoor or highly populated environments such as public transport, additional actions, and time, would be required to find a suitable location, and biometrics will sometimes not be appropriate.

B. Ability to provide a quality sample

With minimal instruction and very little practice, 90% of participants were able to use all of the biometric methods well enough to provide a sample that met the quality criteria. However, there were three participants who could not use one of the biometric modalities. In two cases, the reasons for these failures are not clear, and will be explored in further work. This failure rate underscores the importance of having multiple modalities for authenticating, with a reliable fallback method to support critical access scenarios. The dual conditions had error rates much higher than the sum of the individual error rates. High error rates negate the benefit of dual conditions by increasing the overall time to acquire beyond the time that would be required for single biometrics in sequence. There are multiple possible explanations for the higher error rates. Given the low error rate in the Gesture condition, but high lag time for displaying the gesture, the high error rates for Gesture+Voice may be due to fading off in the voice sample. Poor performance on the Voice+Face condition may be due to the cognitive demand of a task involving two disparate modalities. Practice may reduce these dual condition error rates, but this remains to be empirically tested. In future work, we will examine the quality and consistency of biometric samples provided by the participants, and the performance of verification algorithms on this data set.

C. Impact on the memory recall task

In contrast to prior work that examined password typing time on a mobile device [7], this study presented authentication within a task that demanded short term memory recall. Authentication ‘failure’ due to a poor quality sample, led to a steep drop in task success, from 74% to 47%, confirming the challenge of the task and the disruptive nature of authentication. Perhaps because of this cost of failure,
participants actively employed memory recall strategies to boost their task performance.

Conclusions

We report a laboratory study of the usability of three biometric authentication modalities on a tablet device within the context of a memory task, independent of the performance of biometric verification algorithms. Speaker, face and gesture verification, as well as password entry, were compared using 8-digit written and spoken PIN codes, under six single and dual-biometric conditions. The study identifies usability issues and biometric performance requirements that can serve as a focus for research. Each biometric modality has unique strengths and weaknesses, and has the potential to improve on the Password approach. Face and Voice are fast but not universally usable. Gesture is reliably performed and worked for everyone, but a much shorter gesture would be needed to achieve a competitive time, posing a challenge to gesture recognition algorithms. The memory task context provides further insight into the broader impact of authentication, and demonstrates
a significant advantage for Face, and a lesser advantage for Voice in supporting memory task performance. However, the Voice condition was considered less usable than Password, Face and Gesture. Speaking at a comfortable level did not always meet the voice sample quality threshold, indicating a requirement to operate with a lower threshold. Participants also reported interference with the memory task that was not reflected in their performance. They maintained high performance by using sophisticated memorization strategies, as indicated by their comments and differences in authentication preparation time. Using face recognition also posed challenges for participants, even in good conditions. Careful user interface design is needed to overcome issues with screen reflection and provide feedback for proper alignment.

The conditions that combined two biometric authentication modalities were disliked by the participants, had higher Failure To Acquire and lower performance on the memory recall task. This suggests that combined sample collection for biometric fusion is not necessarily preferable to collecting individual samples. Providing a face or voice biometric to a mobile device seems to be a natural extension of normal device usage requiring no special setup or extra hardware. Software developments such as built-in face recognition are opening further opportunities to streamline the user experience of mobile authentication. This study demonstrates a complex set of trade-offs in selecting and using biometric authentication methods on mobile devices, even in quiet, well-lit conditions. Studies like this one can help to identify critical research challenges for biometric verification algorithms, in addition to design challenges for mobile authentication user interfaces. The goal is to improve on the notoriously cumbersome password method, leading to mobile biometric authentication that is both secure and usable.

References

1. Adams and M. A. Sasse. Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures. *Communications of the ACM*, 42(12):40–46, Dec. 1999.
2. Adobe Systems Inc. PhoneGap. http://phonegap.com.
3. G. Aggarwal, N. K. Ratha, R. M. Bolle, and R. Chellappa. Multi-biometric cohort analysis for biometric fusion. In *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Las Vegas, NV, 2008.
4. E. Altmann and G. Trafton. Task interruption: Disruptive effects and the role of cues. In *Proceedings of the 26th Annual Conference of the Cognitive Science Society*, Chicago, IL, 2004.
5. A. Baddeley and G. Hitch. Working memory. In G. Bower, editor, *Recent Advances in Learning and Motivation*. Academic Press, 1974.
6. A. Bangor, P. T. Kortum, and J. T. Miller. An empirical evaluation of the system usability scale. *International Journal of Human-Computer Interaction*, 2008.
7. P. Bao, J. Pierce, S. Whittaker, and S. Zhai. Smart phone use by non-mobile business users. In *MobileHCI*, Stockholm, Sweden, 2011.
8. J. Basak, K. Kate, V. Tyagi, and N. Ratha. QPLC : A novel multimodal biometric score fusion method. *CVPR Workshop on Biometrics*, 2010.
9. J. Brooke. *SUS: A quick and dirty usability scale*, pages 189–194. Taylor and Francis, 1996.
10. L. Coventry. Usable biometrics. In L. F. Cranor and S. Garfinkel, editors, *Security and Usability: Designing Secure Systems that People can Use*. O'Reilly Books, 2005
11. P. Dunphy, A. P. Heiner, and N. Asokan. A closer look at recognition-based graphical passwords on mobile devices. In *SOUPS*, Redmond,WA, 2010
12. D. Florencio and C. Herley. A large-scale study of web password habits. In *WWW*, Banff, Canada, 2007.
13. D. Florˆencio and C. Herley. Where do security policies come from? In *SOUPS*, Redmond, WA, 2010.
14. N. Gunson, D. Marshall, F. McInnes, and M. Jack. Usability evaluation of voiceprint authentication in automated telephone banking: Sentences versus digits. *Interacting with Computers*, 23(1):57–69, Jan. 2011.
15. T. J. Hazen, E. Weinstein, B. Heisele, A. Park, and J. Ming. Multimodal face and speaker identification for mobile devices. In R. I. Hammoud, B. R. Abidi, and M. A. Abidi, editors, *Face Biometrics for Personal Identification: Multi-Sensory Multi-Modal Systems*. Springer, 2007
16. Y. Ijiri, M. Sakuragi, and S. Lao. Security management for mobile devices by face recognition. In *Proceedings of the 7th International Conference on Mobile Data Management (MDM)*, Nara, Japan, 2006.
17. N. Jackson. Infographic: How Mobile Phones Are Replacing Our Credit Cards, 2011. http://www.theatlantic.com/technology/archive/2011/07/infographic-how-mobile-phones-are-replacingour-credit-cards/241703/.
18. M. Jakobsson, E. Shi, P. Golle, and R. Chow. Implicit authentication for mobile devices. In *HotSec*, Montreal, Canada, 2009.
19. L. A. Jones, A. I. Ant´on, and J. B. Earp. Towards understanding user perceptions of authentication technologies. In *Proceedings of the ACM Workshop on Privacy in Electronic Society*, Alexandria, VA, 2007.
20. S. Krawczyk and A. K. Jain. Securing electronic medical records using biometric authentication. In *Proceedings of the 5th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, Hilton Rye Town, NY, 2005.
21. S. Kurkovsky, T. Carpenter, and C. MacDonald. Experiments with simple iris recognition for mobile phones. In *Proceedings of the 2010 Seventh International Conference on Information Technology: New Generations (ITNG)*, Las Vegas, NV, 2010.
22. M. Lee. Google Turns to Face Detection With Samsung to Take On Apple Speech Parser, 2011. http://www.bloomberg.com/news/2011-10-19/google-turns-to-face-detection-to-take-onapple-iphone-s-speech-technology.html.
23. M. Lennon. One in Three Experience Mobile Device Loss or Theft. Do People in 'Party Cities' Lose More Phones?, 2011. http://www.securityweek.com/ one-three-experience-mobile-device-loss-ortheft- do-people-party-cities-lose-more-phones.
24. S. F. Nagata. Multitasking and interruptions during mobile web tasks. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Denver, CO, 2003.
25. A. Oulasvirta, S. Tamminen, V. Roto, and J. Kuorelahti. Interaction in 4-second bursts: the fragmented nature of attentional resources in mobile hci. In *CHI*, Portland, OR, 2005.
26. N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle. Generating cancelable fingerprint templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):561–572, Apr. 2007.

27. J. Sauro. Measuring usability with the System Usability Scale (SUS), 2011. http://www.measuringusability.com/sus.php.